

**Dell Networking Command-Line Reference
Guide for the Z9500 Switch
Version 9.5(0.1)**



Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 07

Rev. A01

Contents

1 About this Guide.....	42
Objectives.....	42
Audience.....	42
Conventions.....	42
Information Icons.....	43
2 CLI Basics.....	44
Accessing the Command Line.....	44
Multiple Configuration Users.....	44
Obtaining Help.....	45
Navigating the CLI.....	48
Using the Keyword no Command.....	48
Filtering show Commands.....	48
Command Modes.....	49
3 File Management.....	59
boot system.....	59
format flash.....	60
restore factory-defaults.....	61
show boot system.....	62
show bootvar.....	63
show file.....	64
show os-version.....	65
show running-config.....	67
show startup-config.....	70
show version.....	71
upgrade boot.....	73
upgrade fpga-image linecard booted.....	75
upgrade fpga-image system cpld booted.....	77
upgrade fpga-image system fpga booted.....	78
upgrade system.....	79
verify.....	81
4 Control and Monitoring.....	83
asf-mode.....	83
banner exec.....	84
banner login.....	85
banner motd.....	87

cam-acl.....	88
cam-audit linecard.....	89
clear alarms.....	90
clear line.....	91
clear trace.....	92
configure.....	92
debug cpu-traffic-stats.....	93
debug ftpserver.....	94
disable.....	95
do.....	96
enable.....	97
enable optic-info-update interval.....	98
end.....	99
exec-banner.....	100
exec-timeout.....	100
exit.....	101
ftp-server enable.....	103
ftp-server topdir.....	104
ftp-server username.....	105
hostname.....	106
ip ftp password.....	107
ip ftp source-interface.....	108
ip ftp username.....	109
ip http source-interface.....	110
ip telnet server enable.....	111
ip telnet source-interface.....	111
ip tftp source-interface.....	113
line.....	114
logging coredump server.....	115
motd-banner.....	116
ping.....	117
reload.....	121
send.....	121
service timestamps.....	122
show alarms.....	124
show asf.....	126
show command-history.....	127
show command-tree.....	129
show console lp.....	130
show cpu-traffic-stats.....	131
show cpu-interface-stats.....	132
show debugging.....	136

show environment.....	137
show inventory.....	138
show memory.....	140
show processes cpu.....	142
show processes ipc.....	145
show processes ipc flow-control.....	149
show processes memory.....	151
show software ifm.....	157
show system.....	159
show trace.....	161
show tech-support.....	163
show util-threshold cpu.....	166
show util-threshold memory.....	167
system location-led.....	168
telnet.....	169
terminal length.....	170
traceroute.....	171
undebg all.....	173
upload trace-log.....	174
util-threshold cpu.....	175
util-threshold memory.....	176
virtual-ip.....	177
write.....	179

5 802.1X..... 180

debug dot1x.....	181
dot1x auth-fail-vlan.....	181
dot1x auth-server.....	182
dot1x auth-type mab-only.....	183
dot1x authentication (Configuration).....	184
dot1x authentication (Interface).....	185
dot1x guest-vlan.....	185
dot1x host-mode.....	187
dot1x mac-auth-bypass.....	188
dot1x max-eap-req.....	188
dot1x max-suplicants.....	189
dot1x port-control.....	190
dot1x quiet-period.....	191
dot1x reauthentication.....	191
dot1x reauth-max.....	192
dot1x server-timeout.....	193
dot1x supplicant-timeout.....	194

dot1x tx-period.....	195
show dot1x cos-mapping interface.....	196
show dot1x interface.....	197

6 Access Control Lists (ACL)..... 201

Commands Common to all ACL Types.....	201
remark.....	201
show config.....	203
Common IP ACL Commands.....	203
clear counters ip access-group.....	204
ip access-group.....	204
ip control-plane egress-filter.....	206
show ip accounting access-list.....	206
Standard IP ACL Commands.....	208
deny.....	208
ip access-list standard.....	210
permit.....	211
resequence access-list.....	214
resequence prefix-list ipv4.....	215
seq.....	216
Extended IP ACL Commands.....	219
deny.....	219
deny icmp.....	221
deny tcp.....	225
deny udp.....	229
ip access-list extended.....	232
permit.....	233
permit icmp.....	236
permit tcp.....	238
permit udp.....	241
resequence prefix-list ipv4.....	245
seq.....	246
ACL VLAN Group Commands.....	249
acl-vlan-group.....	249
cam-acl-vlan.....	250
description (ACL VLAN Group).....	251
ip access-group (ACL VLAN Group).....	251
member vlan (ACL VLAN Group).....	252
show acl-vlan-group	253
show cam-acl-vlan.....	254
show cam-usage.....	255
show running config acl-vlan-group.....	258

Common MAC ACL Commands.....	259
clear counters mac access-group.....	259
mac access-group.....	260
show mac access-lists.....	262
show mac accounting access-list.....	263
Standard MAC ACL Commands.....	264
deny.....	264
mac access-list standard.....	266
permit.....	267
seq.....	269
Extended MAC ACL Commands.....	271
deny.....	272
mac access-list extended.....	274
permit.....	276
seq.....	278
IP Prefix List Commands.....	280
clear ip prefix-list.....	281
deny.....	281
ip prefix-list.....	283
permit.....	284
seq.....	285
show config.....	286
show ip prefix-list detail.....	287
show ip prefix-list summary.....	288
Route Map Commands.....	289
continue.....	289
description.....	290
match as-path.....	291
match community.....	292
match interface.....	293
match ip address.....	294
match ip next-hop.....	295
match ip route-source.....	296
match metric.....	297
match origin.....	298
match route-type.....	299
match tag.....	300
route-map.....	301
set as-path.....	303
set automatic-tag.....	304
set comm-list delete.....	305
set community.....	306

set level.....	307
set local-preference.....	308
set metric.....	309
set metric-type.....	310
set next-hop.....	311
set origin.....	312
set tag.....	313
set weight.....	314
show config.....	315
show route-map.....	316
AS-Path Commands.....	317
ip as-path access-list.....	317
show ip as-path-access-lists.....	318
IP Community List Commands.....	318
ip community-list.....	319
show ip community-lists.....	319

7 Bidirectional Forwarding Detection (BFD)..... 321

bfd all-neighbors.....	321
bfd disable.....	323
bfd enable (Configuration).....	324
bfd enable (Interface).....	324
bfd interval	325
bfd protocol-liveness.....	326
ip route bfd.....	327
ipv6 ospf bfd all-neighbors.....	328
neighbor bfd.....	329
neighbor bfd disable.....	330
show bfd neighbors.....	332
vrrp bfd.....	333

8 Border Gateway Protocol..... 336

BGP IPv4 Commands.....	336
address-family.....	336
aggregate-address.....	337
bgp add-path.....	339
bgp always-compare-med.....	339
bgp asnotation.....	340
bgp bestpath as-path ignore.....	341
bgp bestpath as-path multipath-relax.....	342
bgp bestpath med confed.....	343
bgp bestpath med missing-as-best.....	344

bgp bestpath router-id ignore.....	344
bgp client-to-client reflection.....	345
bgp cluster-id.....	346
bgp confederation identifier.....	347
bgp confederation peers.....	348
bgp dampening.....	349
bgp default local-preference.....	350
bgp enforce-first-as.....	351
bgp fast-external-fallover.....	352
bgp four-octet-as-support.....	353
bgp graceful-restart.....	354
bgp log-neighbor-changes.....	355
bgp non-deterministic-med.....	356
bgp recursive-bgp-next-hop.....	357
bgp regex-eval-optz-disable.....	358
bgp router-id.....	359
bgp soft-reconfig-backup.....	360
capture bgp-pdu neighbor.....	361
capture bgp-pdu max-buffer-size.....	362
clear ip bgp.....	362
clear ip bgp dampening.....	364
clear ip bgp flap-statistics.....	365
clear ip bgp peer-group.....	366
debug ip bgp.....	367
debug ip bgp dampening.....	368
debug ip bgp events.....	369
debug ip bgp keepalives.....	370
debug ip bgp notifications.....	371
debug ip bgp soft-reconfiguration.....	372
debug ip bgp updates.....	373
default-metric.....	374
description.....	375
distance bgp.....	375
max-paths.....	376
neighbor activate.....	377
neighbor add-path.....	378
neighbor advertisement-interval.....	379
neighbor advertisement-start.....	380
neighbor allowas-in.....	381
neighbor default-originate.....	381
neighbor description.....	382
neighbor distribute-list.....	383

neighbor ebgp-multihop.....	384
neighbor fall-over.....	385
neighbor filter-list.....	386
neighbor graceful-restart.....	387
neighbor local-as.....	388
neighbor maximum-prefix.....	389
neighbor next-hop-self.....	390
neighbor password.....	391
neighbor peer-group (assigning peers).....	392
neighbor peer-group (creating group).....	394
neighbor peer-group passive.....	395
neighbor remote-as.....	396
neighbor remove-private-as.....	397
neighbor route-map.....	398
neighbor route-reflector-client.....	399
neighbor send-community.....	400
neighbor shutdown.....	401
neighbor soft-reconfiguration inbound.....	402
neighbor subnet.....	403
neighbor timers.....	404
neighbor update-source.....	405
neighbor weight.....	406
network.....	407
network backdoor.....	408
redistribute.....	409
redistribute ospf.....	411
router bgp.....	412
show capture bgp-pdu neighbor.....	413
show config.....	414
show ip bgp.....	415
show ip bgp cluster-list.....	417
show ip bgp community.....	418
show ip bgp community-list.....	421
show ip bgp dampened-paths.....	422
show ip bgp detail.....	423
show ip bgp extcommunity-list.....	425
show ip bgp filter-list.....	426
show ip bgp flap-statistics.....	428
show ip bgp inconsistent-as.....	430
show ip bgp neighbors.....	431
show ip bgp next-hop.....	436
show ip bgp paths.....	437

show ip bgp paths as-path.....	439
show ip bgp paths community.....	440
show ip bgp peer-group.....	441
show ip bgp regexp.....	443
show ip bgp summary.....	446
show running-config bgp.....	448
timers bgp.....	449
MBGP Commands.....	450
debug ip bgp dampening.....	450
distance bgp.....	451
show ip bgp dampened-paths.....	452
BGP Extended Communities (RFC 4360).....	453
deny.....	453
deny regex.....	454
description.....	455
ip extcommunity-list.....	455
match extcommunity.....	456
permit.....	457
permit regex.....	458
set extcommunity rt.....	459
set extcommunity soo.....	460
show ip bgp ipv4 extcommunity-list.....	461
show ip bgp paths extcommunity.....	463
show ip extcommunity-list.....	464
show running-config extcommunity-list.....	464
IPv6 BGP Commands.....	465
address-family.....	465
address family ipv6 unicast.....	466
aggregate-address.....	466
bgp always-compare-med.....	468
bgp bestpath as-path ignore.....	468
bgp bestpath med confed.....	469
bgp bestpath med missing-as-best.....	470
bgp client-to-client reflection.....	470
bgp cluster-id.....	471
bgp confederation identifier.....	472
bgp dampening.....	472
bgp default local-preference.....	473
bgp enforce-first-as.....	474
bgp fast-external-fallover.....	475
bgp four-octet-as-support.....	475
bgp graceful-restart.....	476

bgp log-neighbor-changes.....	477
bgp non-deterministic-med.....	477
bgp recursive-bgp-next-hop.....	478
bgp regex-eval-optz-disable.....	479
bgp router-id.....	480
bgp soft-reconfig-backup.....	480
capture bgp-pdu max-buffer-size.....	481
capture bgp-pdu neighbor (ipv6).....	482
clear ip bgp ipv6-address.....	482
clear ip bgp * (asterisk).....	483
clear ip bgp as-number.....	484
clear ip bgp ipv6 dampening.....	485
clear ip bgp ipv6 flap-statistics.....	486
clear ip bgp ipv6 unicast.....	487
clear ip bgp ipv6 unicast dampening.....	488
clear ip bgp ipv6 unicast flap-statistics.....	488
debug ip bgp keepalives.....	489
debug ip bgp ipv6 dampening.....	490
debug ip bgp ipv6 unicast peer-group updates.....	490
debug ip bgp ipv6 unicast dampening.....	491
debug ip bgp ipv6 unicast updates.....	492
debug ip bgp notifications.....	492
debug ip bgp updates.....	493
default-metric.....	494
description.....	495
distance bgp.....	495
ipv6 prefix-list.....	496
maximum-paths.....	497
neighbor activate.....	497
neighbor advertisement-interval.....	498
neighbor allowas-in.....	499
neighbor default-originate.....	500
neighbor description.....	500
neighbor distribute-list.....	501
neighbor ebgp-multihop.....	502
neighbor fall-over.....	503
neighbor filter-list.....	503
neighbor maximum-prefix.....	504
neighbor next-hop-self.....	505
neighbor peer-group (assigning peers).....	506
neighbor peer-group (creating group).....	507
neighbor peer-group passive.....	508

neighbor remote-as.....	508
neighbor remove-private-as.....	509
neighbor route-map.....	510
neighbor route-reflector-client.....	511
neighbor send-community.....	512
neighbor soft-reconfiguration inbound.....	512
neighbor subnet.....	513
neighbor shutdown.....	514
neighbor timers.....	515
neighbor update-source.....	516
neighbor weight.....	517
neighbor X:X:X::X password.....	517
network.....	518
network backdoor.....	519
redistribute.....	520
redistribute ospf.....	521
router bgp.....	522
show capture bgp-pdu neighbor.....	522
show config.....	523
show ip bgp next-hop.....	523
show ip bgp paths.....	524
show ip bgp paths as-path.....	525
show ip bgp paths community.....	525
show ip bgp paths extcommunity.....	526
show ip bgp regexp.....	526
show ipv6 prefix-list.....	527
show ip bgp ipv6 unicast.....	527
show ip bgp ipv6 unicast cluster-list.....	528
show ip bgp ipv6 unicast community.....	529
show ip bgp ipv6 unicast community-list.....	530
show ip bgp ipv6 unicast dampened-paths.....	530
show ip bgp ipv6 unicast detail.....	531
show ip bgp ipv6 unicast extcommunity-list.....	531
show ip bgp ipv6 unicast filter-list.....	532
show ip bgp ipv6 unicast flap-statistics.....	532
show ip bgp ipv6 unicast inconsistent-as.....	533
show ip bgp ipv6 unicast neighbors.....	534
show ip bgp ipv6 unicast peer-group.....	535
show ip bgp ipv6 unicast summary.....	536
timers bgp.....	537
IPv6 MBGP Commands.....	537
show ipv6 mbgproutes.....	537

9 Content Addressable Memory (CAM)	539
CAM Profile Commands	539
cam-acl (Configuration)	539
cam-acl-egress	541
cam-optimization	542
show cam-acl	543
test cam-usage	544
10 Control Plane Policing (CoPP)	547
clear control-traffic protocol	547
clear control-traffic queue	548
control-plane-cpuqos	549
service-policy rate-limit-cpu-queues cpu-qos	550
service-policy rate-limit-protocols cpu-qos	551
show control-traffic protocol	552
show control-traffic queue	554
show cpu-queue rate	556
show ip protocol-queue-mapping	557
show ipv6 protocol-queue-mapping	558
show mac protocol-queue-mapping	559
show protocol-queue-mapping	560
11 Debugging and Diagnostics	564
Offline Diagnostic Commands	564
diag	564
offline system	566
online system	567
show diag	568
show diag information	572
show diag testcase	573
Buffer Tuning Commands	576
buffer-profile (Configuration)	576
Hardware Commands	577
clear control-traffic	577
clear hardware	578
clear hardware system-flow	580
remote-exec	581
show control-traffic	582
show hardware	583
show hardware ipv6	597
show hardware layer2	599

show hardware layer3.....	601
show hardware system-flow.....	603
tcpdump.....	606
12 Dynamic Host Configuration Protocol (DHCP).....	608
Configure a DHCP Server and DHCP Clients	608
clear ip dhcp.....	608
debug ip dhcp client events.....	609
debug ip dhcp client packets.....	610
default-router.....	612
disable.....	612
dns-server.....	613
domain-name.....	614
excluded-address.....	614
hardware-address.....	615
host.....	616
ip address dhcp.....	616
ip address dhcp relay information-option.....	617
ip address dhcp vendor-class-identifier.....	618
lease.....	619
netbios-name-server.....	620
netbios-node-type.....	620
network.....	621
pool.....	622
show ip dhcp client statistics.....	622
show ip dhcp configuration.....	623
show ip dhcp conflict.....	624
show ip dhcp lease.....	625
show ip dhcp server statistics.....	625
Configure Secure DHCP and DHCP Relay.....	626
arp inspection.....	626
arp inspection-trust.....	627
clear ip dhcp snooping.....	628
ip dhcp snooping.....	628
ip dhcp snooping binding.....	629
ip dhcp snooping database.....	630
ip dhcp snooping database renew.....	631
ip dhcp snooping trust.....	631
ip dhcp snooping verify mac-address.....	632
ip dhcp snooping vlan.....	633
ip dhcp source-address-validation.....	633
show ip dhcp binding.....	634

show ip dhcp snooping.....	635
13 Equal Cost Multi-Path (ECMP).....	636
ecmp-group.....	636
hash-algorithm.....	637
hash-algorithm ecmp.....	640
hash-algorithm hg.....	642
hash-algorithm hg-seed.....	643
hash-algorithm seed.....	643
ip ecmp-group.....	644
link-bundle-distribution trigger-threshold.....	645
link-bundle-monitor enable.....	646
show config.....	646
show link-bundle distribution.....	647
14 FIPS Cryptography.....	649
fips mode enable.....	649
show fips status.....	650
show ip ssh.....	650
ssh.....	651
15 Force10 Resilient Ring Protocol (FRRP).....	655
clear frrp.....	655
debug frrp.....	656
description.....	657
disable.....	658
interface.....	659
member-vlan.....	660
mode.....	661
protocol frrp.....	662
show frrp.....	663
timer.....	664
16 GARP VLAN Registration (GVRP).....	666
clear gvrp statistics.....	667
debug gvrp.....	668
disable.....	669
garp timers.....	669
gvrp enable.....	671
gvrp registration.....	672
protocol gvrp.....	673
show config.....	673

show garp timers.....	674
show gvrp.....	675
show gvrp statistics.....	676

17 Internet Group Management Protocol (IGMP)..... 678

IGMP Commands.....	678
clear ip igmp groups.....	678
debug ip igmp.....	679
ip igmp access-group.....	680
ip igmp group-join-limit.....	681
ip igmp immediate-leave.....	682
ip igmp last-member-query-interval.....	683
ip igmp querier-timeout.....	683
ip igmp query-interval.....	684
ip igmp query-max-resp-time.....	685
ip igmp ssm-map.....	686
ip igmp static-group.....	687
ip igmp version.....	688
show ip igmp groups.....	689
show ip igmp interface.....	691
show ip igmp ssm-map.....	692
IGMP Snooping Commands.....	693
ip igmp snooping enable.....	694
ip igmp snooping fast-leave.....	695
ip igmp snooping flood.....	695
ip igmp snooping last-member-query-interval.....	696
ip igmp snooping mrouter.....	697
ip igmp snooping querier.....	698
show ip igmp snooping mrouter.....	699

18 Interfaces..... 701

Basic Interface Commands.....	701
clear counters.....	701
clear dampening.....	703
dampening.....	704
description.....	705
duplex (Management).....	706
flowcontrol.....	707
interface.....	709
interface loopback.....	711
interface ManagementEthernet.....	712
interface null.....	713

interface range.....	714
interface range macro (define).....	717
interface range macro name.....	718
interface vlan.....	719
keepalive.....	720
linecard portmode.....	721
monitor interface.....	722
mtu.....	726
portmode hybrid.....	728
rate-interval.....	730
reset linecard.....	731
show config.....	732
show config (from INTERFACE RANGE mode).....	732
show interfaces.....	733
show interfaces configured.....	740
show interfaces dampening.....	742
show interfaces phy.....	744
show interfaces status.....	746
show interfaces switchport.....	748
show interfaces transceiver.....	750
show range.....	756
show running-config ecmp-group.....	757
shutdown.....	757
speed (Management interface).....	758
switchport.....	759
Egress Interface Selection (EIS) Commands.....	761
application.....	761
clear management application pkt-cntr.....	762
clear management application pkt-fallback-cntr.....	762
management egress-interface-selection.....	763
show ip management-eis-route	763
show management application pkt-cntr.....	764
show management application pkt-fallback-cntr.....	765
Port Channel Commands.....	765
channel-member.....	766
group.....	767
interface port-channel.....	768
minimum-links.....	770
port-channel failover-group.....	770
show config.....	771
show interfaces port-channel.....	772
show port-channel-flow.....	775

HiGig Port Channel Commands.....	777
clear hardware hg-stats.....	778
hg-link-bundle-monitor enable.....	779
hg-link-bundle-monitor rate-interval.....	780
hg-link-bundle-monitor trigger-threshold	780
show hardware hg-stats.....	781
show hg-link-bundle-distribution.....	783
snmp-server enable traps hg-lbm.....	784
UDP Broadcast.....	785
debug ip udp-helper.....	785
ip udp-helper udp-port.....	786
show ip udp-helper.....	787
19 Internet Protocol Security (IPSec).....	789
crypto ipsec transform-set.....	789
crypto ipsec policy.....	791
management crypto-policy.....	792
match.....	792
session-key.....	794
show crypto ipsec transform-set.....	795
show crypto ipsec policy.....	795
transform-set.....	797
20 IPv4 Routing.....	798
arp.....	798
arp backoff-time.....	799
arp learn-enable.....	800
arp retries.....	801
arp timeout.....	801
clear arp-cache.....	802
clear host.....	804
clear ip fib linecard.....	804
clear ip route.....	805
clear ip traffic.....	806
clear tcp statistics.....	807
debug arp.....	808
debug ip dhcp.....	809
debug ip icmp.....	810
debug ip packet.....	812
ip address.....	815
ip directed-broadcast.....	816
ip domain-list.....	816

ip domain-lookup.....	818
ip domain-name.....	819
ip helper-address.....	820
ip helper-address hop-count disable.....	821
ip host.....	822
ip max-frag-count.....	823
ip mtu.....	824
ip name-server.....	825
ip proxy-arp.....	826
ip route.....	827
ip source-route.....	829
ip unreachable.....	830
ipv4 unicast-host-route.....	830
load-balance.....	831
load-balance hg.....	833
management route.....	835
show arp.....	836
show arp retries.....	839
show hosts.....	840
show ip cam linecard.....	842
show ip fib linecard.....	845
show ip flow.....	846
show ip interface.....	848
show ip management-route.....	852
show ipv6 management-route.....	853
show ip protocols.....	854
show ip route.....	855
show ip route list.....	858
show ip route summary.....	859
show ip traffic.....	860
show tcp statistics.....	863

21 IPv6 Access Control Lists (IPv6 ACLs).....867

cam-acl.....	867
cam-acl-egress.....	868
deny (for IPv6 ACLs).....	870
deny arp (for Extended MAC ACLs).....	871
deny icmp (for Extended IPv6 ACLs).....	873
deny tcp (for IPv6 ACLs).....	874
deny udp (for IPv6 ACLs).....	876
ipv6 access-list.....	877
ipv6 control-plane egress-filter.....	878

permit (for IPv6 ACLs).....	879
permit icmp (for IPv6 ACLs).....	880
permit tcp (for IPv6 ACLs).....	882
permit udp (for IPv6 ACLs).....	883
seq (for IPv6 ACLs).....	885
test cam-usage.....	886

22 IPv6 Basics.....889

cam-ipv6 extended-prefix.....	889
clear ipv6 fib.....	890
clear ipv6 route.....	890
clear ipv6 mld_host.....	891
ipv6 address.....	892
ipv6 address eui64.....	893
ipv6 control-plane icmp error-rate-limit.....	894
ipv6 flowlabel-zero.....	895
ipv6 host.....	896
ipv6 name-server.....	896
ipv6 nd dad attempts.....	897
ipv6 nd dns-server	898
ipv6 nd prefix.....	899
ipv6 neighbor.....	900
ipv6 route.....	902
ipv6 unicast-host-route.....	904
ipv6 unicast-routing.....	905
show cam-ipv6 extended-prefix.....	906
show ipv6 cam linecard.....	907
show ipv6 control-plane icmp.....	909
show ipv6 fib linecard.....	910
show ipv6 flowlabel-zero.....	911
show ipv6 interface.....	912
show ipv6 mld_host.....	915
show ipv6 neighbors.....	916
show ipv6 route.....	918

23 Intermediate System to Intermediate System (IS-IS).....921

adjacency-check.....	921
advertise.....	922
area-password.....	923
clear config.....	924
clear isis.....	925
clns host.....	926

debug isis.....	926
debug isis adj-packets.....	927
debug isis local-updates.....	928
debug isis snp-packets.....	929
debug isis spf-triggers.....	930
debug isis update-packets.....	931
default-information originate.....	932
description.....	933
distance.....	934
distribute-list in.....	935
distribute-list out.....	936
distribute-list redistributed-override.....	937
domain-password.....	938
graceful-restart ietf.....	939
graceful-restart interval.....	940
graceful-restart restart-wait.....	941
graceful-restart t1.....	942
graceful-restart t2.....	943
graceful-restart t3.....	943
hello padding.....	945
hostname dynamic.....	946
ignore-lsp-errors.....	946
ip router isis.....	947
ipv6 router isis.....	948
isis circuit-type.....	949
isis csnp-interval.....	950
isis hello-interval.....	951
isis hello-multiplier.....	952
isis hello padding.....	953
isis ipv6 metric.....	954
isis metric.....	955
isis network point-to-point.....	956
isis password.....	957
isis priority.....	958
is-type.....	959
log-adjacency-changes.....	960
lsp-gen-interval.....	960
lsp-mtu.....	962
lsp-refresh-interval.....	963
max-area-addresses.....	964
max-lsp-lifetime.....	964
maximum-paths.....	965

metric-style.....	966
multi-topology.....	967
net.....	968
passive-interface.....	969
redistribute.....	970
redistribute bgp.....	972
redistribute ospf.....	974
router isis.....	975
set-overload-bit.....	976
show config.....	977
show isis database.....	978
show isis graceful-restart detail.....	981
show isis hostname.....	982
show isis interface.....	983
show isis neighbors.....	984
show isis protocol.....	986
show isis traffic.....	987
spf-interval.....	989

24 Link Aggregation Control Protocol (LACP)..... 991

clear lacp counters.....	991
debug lacp.....	992
lacp long-timeout.....	993
lacp port-priority.....	994
lacp system-priority.....	995
port-channel mode.....	995
port-channel-protocol lacp.....	997
show lacp.....	997

25 Layer 2..... 1000

MAC Addressing Commands.....	1000
clear mac-address-table.....	1000
mac-address-table aging-time.....	1001
mac-address-table static.....	1002
mac-address-table station-move refresh-arp.....	1004
mac learning-limit.....	1004
mac learning-limit learn-limit-violation.....	1006
mac learning-limit mac-address-sticky.....	1007
mac learning-limit station-move-violation.....	1008
mac learning-limit reset.....	1009
show cam mac linecard (dynamic or static).....	1009
show mac-address-table.....	1011

show mac-address-table aging-time.....	1014
show mac learning-limit.....	1015
Virtual LAN (VLAN) Commands.....	1016
default vlan-id.....	1016
default-vlan disable.....	1017
name.....	1018
show config.....	1019
show vlan.....	1019
tagged.....	1023
track ip.....	1024
untagged.....	1025
Far-End Failure Detection (FEFD).....	1026
debug fefd.....	1026
fefd.....	1027
fefd disable.....	1028
fefd interval.....	1029
fefd mode.....	1030
fefd reset.....	1031
fefd-global interval.....	1031
fefd-global.....	1032
show fefd.....	1033

26 Link Layer Discovery Protocol (LLDP).....1036

LLPD Commands.....	1036
advertise dot1-tlv.....	1036
advertise dot3-tlv.....	1037
advertise management-tlv.....	1038
advertise management-tlv (Interface).....	1039
clear lldp counters.....	1040
clear lldp neighbors.....	1041
debug lldp interface.....	1041
disable.....	1043
hello.....	1044
management-interface.....	1044
mode.....	1045
multiplier.....	1046
protocol lldp (Configuration).....	1047
protocol lldp (Interface).....	1047
show lldp neighbors.....	1048
show lldp statistics.....	1049
show management-interface.....	1050
show running-config lldp.....	1050

LLDP-MED Commands.....	1051
advertise med guest-voice.....	1052
advertise med guest-voice-signaling.....	1053
advertise med location-identification.....	1054
advertise med power-via-mdi.....	1055
advertise med softphone-voice.....	1056
advertise med streaming-video.....	1057
advertise med video-conferencing.....	1058
advertise med video-signaling.....	1059
advertise med voice.....	1060
advertise med voice-signaling.....	1061
27 Microsoft Network Load Balancing.....	1062
arp (for Multicast MAC Address).....	1062
ip vlan-flooding.....	1063
mac-address-table static (for Multicast MAC Address).....	1064
28 Multicast.....	1066
IPv4 Multicast Commands.....	1066
clear ip mroute.....	1066
ip mroute.....	1067
ip multicast-limit.....	1068
ip multicast-routing.....	1069
show ip mroute.....	1070
show ip rpf.....	1073
IPv6 Multicast Commands.....	1073
debug ipv6 mld_host.....	1074
ip multicast-limit.....	1075
29 Multicast Source Discovery Protocol (MSDP).....	1076
clear ip msdp peer.....	1076
clear ip msdp sa-cache.....	1077
clear ip msdp statistic.....	1078
debug ip msdp.....	1079
ip msdp cache-rejected-sa.....	1079
ip msdp default-peer.....	1080
ip msdp log-adjacency-changes.....	1081
ip msdp mesh-group.....	1082
ip msdp originator-id.....	1083
ip msdp peer.....	1084
ip msdp redistribute.....	1085
ip msdp sa-filter.....	1086

ip msdp sa-limit.....	1087
ip msdp shutdown.....	1088
ip multicast-msdp.....	1089
show ip msdp.....	1089
show ip msdp sa-cache rejected-sa.....	1091

30 Multiple Spanning Tree Protocol (MSTP).....1092

debug spanning-tree mstp.....	1092
disable.....	1093
forward-delay.....	1094
hello-time.....	1095
max-age.....	1096
max-hops.....	1097
msti.....	1098
name.....	1099
protocol spanning-tree mstp.....	1100
revision.....	1101
show config.....	1102
show spanning-tree mst configuration.....	1102
show spanning-tree msti.....	1103
spanning-tree.....	1106
spanning-tree msti.....	1107
spanning-tree mstp edge-port.....	1108
tc-flush-standard.....	1109

31 Open Shortest Path First (OSPFv2 and OSPFv3).....1111

OSPFv2 Commands.....	1111
area default-cost.....	1111
area nssa.....	1112
area range.....	1113
area stub.....	1114
auto-cost.....	1115
clear ip ospf.....	1116
clear ip ospf statistics.....	1117
debug ip ospf.....	1118
default-information originate.....	1120
default-metric.....	1121
description.....	1122
distance.....	1123
distance ospf.....	1124
distribute-list in.....	1125
distribute-list out.....	1126

enable inverse-mask.....	1127
fast-convergence.....	1128
flood-2328.....	1129
graceful-restart grace-period.....	1130
graceful-restart helper-reject.....	1130
graceful-restart mode.....	1131
graceful-restart role.....	1132
ip ospf auth-change-wait-time.....	1133
ip ospf authentication-key.....	1134
ip ospf cost.....	1134
ip ospf dead-interval.....	1135
ip ospf hello-interval.....	1136
ip ospf message-digest-key.....	1137
ip ospf mtu-ignore.....	1138
ip ospf network.....	1139
ip ospf priority.....	1140
ip ospf retransmit-interval.....	1140
ip ospf transmit-delay.....	1141
log-adjacency-changes.....	1142
maximum-paths.....	1143
mib-binding.....	1144
network area.....	1144
passive-interface.....	1146
redistribute.....	1148
redistribute bgp.....	1149
redistribute isis.....	1150
router-id.....	1151
router ospf.....	1152
show config.....	1153
show ip ospf.....	1154
show ip ospf asbr.....	1156
show ip ospf database.....	1157
show ip ospf database asbr-summary.....	1159
show ip ospf database external.....	1161
show ip ospf database network.....	1163
show ip ospf database nssa-external.....	1165
show ip ospf database opaque-area.....	1166
show ip ospf database opaque-as.....	1169
show ip ospf database opaque-link.....	1170
show ip ospf database router.....	1171
show ip ospf database summary.....	1173
show ip ospf interface.....	1176

show ip ospf neighbor.....	1178
show ip ospf routes.....	1179
show ip ospf statistics.....	1180
show ip ospf timers rate-limit.....	1184
show ip ospf topology.....	1185
summary-address.....	1186
timers spf.....	1187
timers throttle lsa all.....	1188
timers throttle lsa arrival.....	1189
OSPFv3 Commands.....	1190
area authentication.....	1190
area encryption.....	1191
clear ipv6 ospf process.....	1194
debug ipv6 ospf bfd.....	1194
debug ipv6 ospf packet.....	1196
default-information originate.....	1197
graceful-restart grace-period.....	1198
graceful-restart mode.....	1199
ipv6 ospf area.....	1200
ipv6 ospf authentication.....	1201
ipv6 ospf bfd all-neighbors.....	1202
ipv6 ospf cost.....	1204
ipv6 ospf dead-interval.....	1204
ipv6 ospf encryption.....	1205
ipv6 ospf graceful-restart helper-reject.....	1207
ipv6 ospf hello-interval.....	1208
ipv6 ospf priority.....	1209
ipv6 router ospf.....	1209
maximum-paths.....	1210
passive-interface.....	1211
redistribute.....	1212
router-id.....	1214
show crypto ipsec policy.....	1215
show crypto ipsec sa ipv6.....	1217
show ipv6 ospf interface.....	1219
show ipv6 ospf database.....	1220
show ipv6 ospf neighbor.....	1222

32 Pay As You Grow 1224

install license.....	1224
show license.....	1226

33 PIM-Sparse Mode (PIM-SM).....	1228
IPv4 PIM-Sparse Mode Commands.....	1228
clear ip pim rp-mapping.....	1228
clear ip pim tib.....	1229
debug ip pim.....	1229
ip pim bsr-border.....	1231
ip pim bsr-candidate.....	1231
ip pim dr-priority.....	1233
ip pim join-filter.....	1233
ip pim ingress-interface-map.....	1235
ip pim neighbor-filter.....	1235
ip pim query-interval.....	1236
ip pim register-filter.....	1237
ip pim rp-address.....	1238
ip pim rp-candidate.....	1239
ip pim sparse-mode.....	1240
ip pim sparse-mode sg-expiry-timer.....	1241
ip pim spt-threshold.....	1242
no ip pim snooping dr-flood.....	1242
show ip pim bsr-router.....	1243
show ip pim interface.....	1244
show ip pim neighbor.....	1245
show ip pim rp.....	1247
show ip pim snooping interface.....	1248
show ip pim snooping neighbor.....	1249
show ip pim snooping tib.....	1250
show ip pim summary.....	1252
show ip pim tib.....	1254
show running-config pim.....	1256
IPv6 PIM-Sparse Mode Commands.....	1256
clear ipv6 pim tib.....	1257
ipv6 pim bsr-border.....	1257
ipv6 pim bsr-candidate.....	1258
ipv6 pim dr-priority.....	1259
ipv6 pim join-filter.....	1260
ipv6 pim neighbor-filter.....	1261
ipv6 pim query-interval.....	1262
ipv6 pim register-filter.....	1262
ipv6 pim rp-address.....	1263
ipv6 pim rp-candidate.....	1264
ipv6 pim sparse-mode.....	1265

ipv6 pim spt-threshold.....	1266
show ipv6 pim bsr-router.....	1266
show ipv6 pim interface.....	1267
show ipv6 pim neighbor.....	1268
show ipv6 pim rp.....	1268
show ipv6 pim tib.....	1270
34 PIM-Source Specific Mode (PIM-SSM).....	1272
IPv4 PIM Commands.....	1272
IPv4 PIM-Source Specific Mode Commands.....	1272
ip pim ssm-range.....	1272
show ip pim ssm-range.....	1274
IPv6 PIM Commands.....	1274
IPv6 PIM-Source Specific Mode Commands.....	1275
ipv6 pim ssm-range.....	1275
show ipv6 pim ssm-range.....	1276
35 Policy-based Routing (PBR).....	1277
description.....	1277
ip redirect-group.....	1278
ip redirect-list.....	1279
permit.....	1280
redirect.....	1281
seq.....	1283
show cam pbr.....	1285
show ip redirect-list.....	1286
36 Port Monitoring.....	1288
description.....	1288
monitor session.....	1289
show config.....	1290
show monitor session.....	1291
show running-config monitor session.....	1292
source (port monitoring).....	1293
37 Private VLAN (PVLAN).....	1296
ip local-proxy-arp.....	1297
private-vlan mode.....	1298
private-vlan mapping secondary-vlan.....	1299
show interfaces private-vlan.....	1301
show vlan private-vlan.....	1302
switchport mode private-vlan.....	1305

38 Per-VLAN Spanning Tree Plus (PVST+).....	1307
description.....	1307
disable.....	1308
extend system-id.....	1308
protocol spanning-tree pvst.....	1309
show spanning-tree pvst.....	1311
spanning-tree pvst.....	1314
spanning-tree pvst err-disable.....	1317
tc-flush-standard.....	1317
vlan bridge-priority.....	1318
vlan forward-delay.....	1319
vlan hello-time.....	1320
vlan max-age.....	1321
 39 Quality of Service (QoS).....	 1323
Global Configuration Commands.....	1323
qos-rate-adjust.....	1323
service-class bandwidth-percentage.....	1324
service-class dot1p-mapping.....	1325
service-class dynamic dot1p.....	1325
service-class wred backplane.....	1327
service-class wred ecn backplane.....	1328
service-pool wred.....	1329
show qos dot1p-queue-mapping.....	1331
Per-Port QoS Commands.....	1331
dot1p-priority.....	1332
rate police.....	1333
rate shape.....	1334
strict-priority	1335
Policy-Based QoS Commands.....	1336
bandwidth-percentage.....	1336
class-map.....	1337
clear qos statistics.....	1339
description.....	1339
match ip access-group.....	1340
match ip dscp.....	1341
match ip precedence.....	1343
match ip vlan.....	1344
match mac access-group.....	1345
match mac dot1p.....	1346
match mac vlan.....	1347

policy-aggregate.....	1347
policy-map-input.....	1348
policy-map-output.....	1349
qos-policy-input.....	1350
qos-policy-output.....	1352
rate-police.....	1353
rate-shape.....	1354
service-policy input.....	1355
service-policy output.....	1356
service-queue.....	1357
set.....	1358
show qos class-map.....	1359
show qos policy-map.....	1360
show qos policy-map-input.....	1362
show qos policy-map-output.....	1363
show qos qos-policy-input.....	1364
show qos qos-policy-output.....	1365
show qos statistics.....	1365
show qos wred-profile.....	1367
test cam-usage.....	1368
threshold.....	1370
trust.....	1371
wred.....	1373
wred weight.....	1374
wred ecn.....	1374
wred-profile.....	1375
DSCP Color Map Commands.....	1376
dscp.....	1376
qos dscp-color-map.....	1378
qos dscp-color-policy.....	1379
show qos dscp-color-map	1379

40 Routing Information Protocol (RIP)..... 1381

auto-summary.....	1381
clear ip rip.....	1382
debug ip rip.....	1382
default-information originate.....	1383
default-metric.....	1384
description.....	1385
distance.....	1386
distribute-list in.....	1387
distribute-list out.....	1388

ip poison-reverse.....	1389
ip rip receive version.....	1390
ip rip send version.....	1391
ip split-horizon.....	1392
maximum-paths.....	1393
neighbor.....	1394
network.....	1395
offset-list.....	1396
output-delay.....	1397
passive-interface.....	1398
redistribute.....	1399
redistribute isis.....	1400
redistribute ospf.....	1401
router rip.....	1402
show config.....	1403
show ip rip database.....	1403
show running-config rip.....	1405
timers basic.....	1406
version.....	1407

41 Remote Monitoring (RMON).....1409

rmon alarm.....	1409
rmon collection history.....	1411
rmon collection statistics.....	1412
rmon event.....	1413
rmon hc-alarm.....	1414
show rmon.....	1415
show rmon alarms.....	1416
show rmon events.....	1418
show rmon hc-alarm.....	1419
show rmon history.....	1420
show rmon log.....	1421
show rmon statistics.....	1422

42 Rapid Spanning Tree Protocol (RSTP).....1425

bridge-priority.....	1425
debug spanning-tree rstp.....	1426
description.....	1427
disable.....	1428
forward-delay.....	1429
hello-time.....	1430
max-age.....	1431

protocol spanning-tree rstp.....	1432
show config.....	1433
show spanning-tree rstp.....	1433
spanning-tree rstp.....	1436
tc-flush-standard.....	1438

43 Security.....1439

Role-Based Access Control Commands.....	1439
aaa authorization role-only	1440
role	1441
show role	1442
show userroles	1443
userrole	1443
AAA Accounting Commands.....	1444
aaa accounting.....	1445
aaa accounting suppress.....	1447
accounting.....	1447
show accounting.....	1449
Authorization and Privilege Commands.....	1450
authorization.....	1450
aaa authorization commands.....	1451
aaa authorization config-commands.....	1452
aaa authorization exec.....	1453
privilege level (CONFIGURATION mode).....	1454
privilege level (LINE mode).....	1455
Authentication and Password Commands.....	1456
aaa authentication enable.....	1456
aaa authentication login.....	1457
access-class.....	1459
enable password.....	1460
enable restricted.....	1462
enable secret.....	1463
login authentication.....	1464
password.....	1465
password-attributes.....	1466
service password-encryption.....	1468
show privilege.....	1469
show users.....	1470
timeout login response.....	1471
username.....	1472
RADIUS Commands.....	1474
debug radius.....	1474

ip radius source-interface.....	1474
radius-server deadtime.....	1475
radius-server host.....	1476
radius-server key.....	1478
radius-server retransmit.....	1479
radius-server timeout.....	1480
TACACS+ Commands.....	1481
debug tacacs+.....	1481
ip tacacs source-interface.....	1481
tacacs-server host.....	1482
tacacs-server key.....	1484
Port Authentication (802.1X) Commands.....	1485
dot1x authentication (Configuration).....	1485
dot1x authentication (Interface).....	1486
dot1x auth-fail-vlan.....	1487
dot1x auth-server.....	1488
dot1x guest-vlan.....	1488
dot1x mac-auth-bypass.....	1489
dot1x max-eap-req.....	1490
dot1x port-control.....	1491
dot1x quiet-period.....	1491
dot1x reauthentication.....	1492
dot1x reauth-max.....	1493
dot1x server-timeout.....	1494
dot1x supplicant-timeout.....	1494
dot1x tx-period.....	1495
show dot1x interface.....	1496
SSH Server and SCP Commands.....	1497
crypto key generate.....	1497
crypto key zeroize rsa.....	1498
debug ip ssh.....	1499
ip scp topdir.....	1500
ip ssh authentication-retries.....	1501
ip ssh connection-rate-limit.....	1501
ip ssh hostbased-authentication.....	1502
ip ssh key-size.....	1503
ip ssh password-authentication.....	1504
ip ssh pub-key-file.....	1505
ip ssh rekey	1506
ip ssh rhostsfile.....	1507
ip ssh rsa-authentication (Config).....	1508
ip ssh rsa-authentication (EXEC).....	1509

ip ssh server.....	1510
ip ssh source-interface.....	1513
show crypto.....	1514
show ip ssh.....	1515
show ip ssh client-pub-keys.....	1516
show ip ssh rsa-authentication.....	1517
ssh.....	1518
Secure DHCP Commands.....	1520
clear ip dhcp snooping.....	1521
ip dhcp relay.....	1521
ip dhcp snooping.....	1522
ip dhcp snooping binding.....	1523
ip dhcp snooping database.....	1524
ip dhcp snooping database renew.....	1524
ip dhcp snooping trust.....	1525
ip dhcp source-address-validation.....	1525
ip dhcp snooping vlan.....	1526
show ip dhcp snooping.....	1527
44 Service Provider Bridging.....	1528
debug protocol-tunnel.....	1528
protocol-tunnel.....	1529
protocol-tunnel destination-mac.....	1530
protocol-tunnel enable.....	1531
protocol-tunnel rate-limit.....	1532
show protocol-tunnel.....	1533
45 sFlow.....	1535
sflow collector.....	1536
sflow enable (Global).....	1537
sflow enable (Interface).....	1538
sflow extended-switch enable.....	1539
sflow polling-interval (Global).....	1540
sflow polling-interval (Interface).....	1541
sflow sample-rate (Global).....	1542
sflow sample-rate (Interface).....	1543
show sflow.....	1544
show sflow linecard.....	1546
46 Simple Network Management Protocol (SNMP) and Syslog.....	1548
SNMP Commands.....	1548
show snmp.....	1549

show snmp engineID.....	1550
show snmp group.....	1550
show snmp user.....	1551
snmp ifmib ifalias long.....	1552
snmp-server community.....	1553
snmp-server contact.....	1555
snmp-server enable traps.....	1556
snmp-server engineID.....	1558
snmp-server group.....	1559
snmp-server host.....	1561
snmp-server location.....	1564
snmp-server packetsize.....	1565
snmp-server trap-source.....	1566
snmp-server user.....	1567
snmp-server view.....	1569
snmp trap link-status.....	1570
Syslog Commands.....	1571
clear logging.....	1571
clear logging auditlog.....	1572
default logging buffered.....	1572
default logging console.....	1573
default logging monitor.....	1574
default logging trap.....	1574
logging.....	1575
logging buffered.....	1576
logging console.....	1577
logging extended.....	1578
logging facility.....	1579
logging history.....	1580
logging history size.....	1581
logging monitor.....	1582
logging on.....	1583
logging source-interface.....	1584
logging synchronous.....	1585
logging trap.....	1586
logging version.....	1587
show logging.....	1588
show logging auditlog.....	1590
show logging driverlog.....	1590
show logging kernellog.....	1592
terminal monitor.....	1594

47 SNMP Traps.....	1596
48 Storm Control.....	1600
show storm-control broadcast.....	1600
show storm-control multicast.....	1601
show storm-control unknown-unicast.....	1602
storm-control broadcast (Configuration).....	1603
storm-control broadcast (Interface).....	1604
storm-control multicast (Configuration).....	1605
storm-control multicast (Interface).....	1606
storm-control unknown-unicast (Configuration).....	1606
storm-control unknown-unicast (Interface).....	1607
49 Spanning Tree Protocol (STP).....	1609
bpdu-destination-mac-address.....	1609
bridge-priority.....	1610
debug spanning-tree.....	1610
description.....	1612
disable.....	1612
forward-delay.....	1613
hello-time.....	1614
max-age.....	1615
protocol spanning-tree.....	1616
show config.....	1617
show spanning-tree 0.....	1618
spanning-tree 0.....	1621
50 System Time and Date.....	1624
calendar set.....	1624
clock read-calendar.....	1625
clock set.....	1626
clock summer-time date.....	1627
clock summer-time recurring.....	1629
clock timezone.....	1631
debug ntp.....	1632
ntp authenticate.....	1633
ntp authentication-key.....	1634
ntp broadcast client.....	1635
ntp disable.....	1636
ntp multicast client.....	1636
ntp server.....	1637

ntp source.....	1638
ntp trusted-key.....	1639
ntp update-calendar.....	1640
show calendar.....	1641
show clock.....	1642
show ntp associations.....	1643
show ntp status.....	1644
51 Tunneling Commands.....	1646
ip unnumbered.....	1646
ipv6 unnumbered.....	1647
tunnel allow-remote.....	1648
tunnel destination.....	1649
tunnel dscp.....	1649
tunnel flow-label.....	1650
tunnel hop-limit.....	1651
tunnel mode.....	1652
tunnel source.....	1653
52 Uplink Failure Detection (UFD).....	1655
clear ufd-disable.....	1655
debug uplink-state-group.....	1656
description.....	1657
downstream.....	1657
downstream auto-recover.....	1659
downstream disable links.....	1660
enable.....	1661
show running-config uplink-state-group.....	1661
show uplink-state-group.....	1662
uplink-state-group.....	1664
upstream.....	1665
53 VLAN Stacking.....	1667
member.....	1668
vlan-stack access.....	1669
vlan-stack compatible.....	1669
vlan-stack dot1p-mapping.....	1671
vlan-stack protocol-type.....	1671
vlan-stack trunk.....	1673
54 Virtual Link Trunking (VLT).....	1676
back-up destination.....	1676

clear vlt statistics.....	1677
delay-restore.....	1678
lacp ungroup member-independent.....	1679
multicast peer-routing timeout.....	1681
peer-link port-channel.....	1681
peer-routing.....	1682
peer-routing-timeout.....	1683
primary-priority.....	1684
show vlt brief.....	1684
show vlt backup-link.....	1685
show vlt counters.....	1686
show vlt detail.....	1688
show vlt inconsistency.....	1689
show vlt mismatch.....	1689
show vlt private-vlan.....	1690
show vlt role.....	1691
show vlt statistics.....	1692
show vlt statistics igmp-snoop.....	1694
system-mac.....	1695
unit-id.....	1695
vlt domain.....	1696
vlt-peer-lag port-channel.....	1697

55 VLT Proxy Gateway.....1699

proxy-gateway lldp.....	1699
proxy-gateway static.....	1700
remote-mac-address exclude-vlan.....	1700
peer-domain-link port-channel exclude-vlan.....	1701
proxy-gateway peer-timeout	1702
vlt-peer-mac transmit.....	1703
show vlt-proxy-gateway.....	1703

56 Virtual Router Redundancy Protocol (VRRP).....1705

IPv4 VRRP Commands.....	1705
advertise-interval.....	1705
authentication-type.....	1706
clear counters vrrp.....	1707
debug vrrp.....	1708
description.....	1709
disable.....	1710
hold-time.....	1710
preempt.....	1711

priority.....	1712
show config.....	1713
show vrrp.....	1714
version	1717
virtual-address.....	1718
vrrp delay minimum.....	1719
vrrp delay reload.....	1720
vrrp-group.....	1721
IPv6 VRRP Commands.....	1722
clear counters vrrp ipv6.....	1722
debug vrrp ipv6.....	1723
show vrrp ipv6.....	1724
vrrp-ipv6-group.....	1726

About this Guide

This book provides information about the Dell Networking operating system (OS) command line interface (CLI).

This book also includes information about the protocols and features supported in the Dell Networking OS on the Z9500 switch.

References

For more information about your system, refer to the following documents:

- *Dell Networking Z9500 Getting Started Guide*
- *Dell Networking Z9500 Installation Guide*
- *Dell Networking Z9500 Configuration Guide*
- *Dell Networking Z9500 Release Notes*

Objectives

This book is intended as a reference guide for CLI commands in the Dell Networking OS running on the Z9500, with detailed syntax statements, usage information and sample output.



NOTE: For more information about when to use the CLI commands, refer to the *Z9500 Configuration Guide* for your system.

Audience

This book is intended for system administrators who are responsible for configuring or maintaining networks. This guide assumes that you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

This book uses the following conventions to describe command syntax.

Keyword

Keywords are in Courier and must be entered in the CLI as listed.

<i>parameter</i>	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.
x y	Keywords and parameters separated by a bar require you to choose one option.
x y	Keywords and parameters separated by a double bar allows you to choose any or all of the options.

Information Icons

This book uses the following information symbols:



NOTE: The Note icon signals important operational information.



CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.



WARNING: The Warning icon signals information about hardware handling that could result in injury.

CLI Basics

This chapter describes the command line interface (CLI) structure and command modes. Dell Networking OS commands are in a text-based interface that allows you to use the launch commands, change command modes, and configure interfaces and protocols.

Accessing the Command Line

When the system boots successfully, you are positioned on the command line in EXEC mode and not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into the switch, you are prompted to enter a login name and password.

Example

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password: Dell>
```

After you log in to the switch, the prompt provides you with the current command-level information. For example:

Prompt	CLI Command Mode
Dell>	EXEC
Dell#	EXEC Privilege
Dell(conf)#	CONFIGURATION



NOTE: For a list of all the command mode prompts, refer to the [Command Modes](#) section.

Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, the Dell Networking OS generates an alert warning message similar to the following:

```
Dell#conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )
Dell#conf
```


When another user enters CONFIGURATION mode, the system sends a message similar to the following:

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

In this case, the user is "admin" on vty2.

Obtaining Help

As soon as you are in a command mode there are several ways to access help.

To obtain a list of keywords at any command mode:	Type a ? at the prompt or after a keyword. There must always be a space before the ?.
--	---

To obtain a list of keywords with a brief functional description:	Type help at the prompt.
--	--------------------------

To obtain a list of available options:	Type a keyword and then type a space and a ?.
---	---

To obtain a list of partial keywords using a partial keyword:	Type a partial keyword and then type a ?.
--	---

Example	The following is an example of typing ip ? at the prompt:
----------------	---

Dell(conf)# ?	
aaa	Authentication, Authorization
and Accounting	
arp	Set a static ARP entry
asf-mode	Enable Cut-Thru Mode
banner	Define a login banner
bfd	Configure BFD protocol
boot	Modify system boot parameters
bpdu-destination-mac-address	Use Provider Bridge Address
for xStp/Gvrp	
cam-acl	Configure CAM ACL
cam-audit	Configure CAM auditing
parameters	
cam-acl-egress	Configure Egress CAM ACL
cam-optimization	Optimize Cam utilization
class-map	Configure Class Map for QoS
clock	Configure time-of-day clock
configuration	Enables exclusive
configuration mode	
crypto	SSH key generation and IPSec
policy configuration	
control-plane-cpuqos	Control plane CPU Qos
configuration	
default	Set a command to its default
default-vlan	Change flooding on default vlan
define	Interface range macro

definition	
dot1x	Configure 802.1x
ecmp-group	ECMP group configuration
enable	Modify enable password
parameters	
end	Exit from configuration mode
ethernet	Ethernet options
exit	Exit from configuration mode
fastpatch	Process runtime patch
fejd-global	Enable FEJD globally
ftp-server	FTP configuration subcommands
garp	Configure GARP parameters
hash-algorithm	Hash algorithm command
hg-link-bundle-monitor	Configure HiGig Link Bundle
Monitoring	
hostname	Set system's network name
http-server	Configure the HTTP server
interface	Select an interface to
configure	
ip	Global IP configuration
subcommands	
ipv6	Global IPv6 configuration
subcommands	
lACP	Configure LACP
line	Configure a terminal line
linecard	Configure linecard
link-bundle-distribution	Configure link-bundle
load-balance	Global traffic load-balance
configuration	
logging	Modify message logging
facilities	
mac	Global MAC configuration
subcommands	
mac-address-table	Mac Address Table
Configuration Subcommands	
management	Create a management crypto or
route, etc	
monitor	Monitor monitored ports
no	Reset a command
ntp	Configure NTP
openflow	Configure OpenFlow instance
password-attributes	Configure password attributes
policy-map-input	Configure input QoS policy map
policy-map-output	Configure output QoS policy map
port-channel	Configure port-channel group
parameters	
privilege	Command privilege parameters
protocol	Select a protocol to configure
protocol-tunnel	Configure protocol tunneling
qos-policy-input	Configure input QoS policy
qos-policy-output	Configure output QoS policy
qos-rate-adjust	Configure the number of bytes
added to each frame for rate policing/shaping	
radius-server	Set up RADIUS server
redundancy	Set up linecard redundancy
configuration	
reload-type	Configure the reload type
rmon	Configure RMON alarm/event
tables	
route-map	Create route-map or enter
route-map command mode	
router	Enable a routing process
script	Start or stop a script
service	Service selected component

service-class	Define service class to policy
based QoS/Routing mapping	
sflow	sFlow configuration
snmp	Modify SNMP parameters
snmp-server	Modify SNMP parameters
storm-control	Configure storm-control
strict-priority	Configure a Queue as a strict
priority queue	
switch	Configure Script CPU and
Memory Limits	
mount	Mount target directory
tacacs-server	Set up TACACS+ server
uplink-state-group	Uplink state group creation
and configurations	
username	Establish user name
authentication	
util-threshold	Cpu or memory utilization
configurations	
virtual-ip	Virtual IP address
vlan-stack	Vlan-stack command
vlt	Enable Virtual Link Trunk
wred-profile	Create a WRED profile

When entering commands, you can take advantage of the following timesaving features:

- The commands are not case-sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int ten 0/1` for the interface `tengigabitethernet 0/1` command.
- To complete keywords in commands, use the TAB key.
- To display the last enabled command, use the up Arrow key.
- Use either the Backspace key or Delete key to erase the previous character.
- To navigate left or right in the command line, use the left and right Arrow keys.

The shortcut key combinations at the command line are as follows:

Key Combination	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes the character at the cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.
CNTL-I	Completes a keyword.
CNTL-K	Deletes all the characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Returns to the more recent commands in the history buffer after recalling commands with Ctrl-P or the up Arrow key.
CNTL-P	Recalls commands, beginning with the last command.
CNTL-R	Re-enters the previous command.

Key Combination	Action
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of the command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all the characters from the cursor to the end of the word.

Navigating the CLI

The Dell Networking OS displays a CLI prompt comprised of the host name and CLI mode.

- Host name is the initial part of the prompt and is “Dell” by default. You can change the host name with the `hostname` command.
- CLI mode is the second part of the prompt and reflects the current CLI mode. For a list of the Dell Networking OS command modes, refer to the command mode list in the [Accessing the Command Line](#) section.

The CLI prompt changes as you move up and down the levels of the command structure. Starting with CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. For more information about command modes, refer to the [Command Modes](#) section.

Using the Keyword `no` Command

To disable, delete or return to default values, use the `no` form of the commands.

For most commands, if you type the keyword `no` in front of the command, you disable that command or delete it from the running configuration. In this guide, the `no` form of the command is described in the Syntax portion of the command description.

Filtering `show` Commands

To find specific information, display certain information only or begin the command output at the first instance of a regular expression or phrase, you can filter the display output of a `show` command.

When you execute a `show` command, and then enter a pipe (`|`), one of the following parameters, and a regular expression, the resulting output either excludes or includes those parameters.

 **NOTE:** You can enter a space before or after the pipe, no space before or after the pipe, or any combination. For example: `Dell#command | grep fortyGigE |except regular-expression | find regular-expression`

display	displays additional configuration information						
except	displays only the text that does not match the pattern (or regular expression)						
find	searches for the first occurrence of a pattern						
grep	displays text that matches a pattern. The <code>grep</code> command option has an <code>ignore-case</code> suboption that makes the search case-insensitive. For example, the commands: <table border="0" data-bbox="478 472 1396 829"> <tr> <td>show run grep Ethernet</td><td>returns a search result with instances containing a capitalized "Ethernet," such as <code>interface fortyGigE 0/0</code></td></tr> <tr> <td>show run grep ethernet</td><td>does not return the previous search result because it only searches for instances containing a noncapitalized "ethernet"</td></tr> <tr> <td>show run grep Ethernet ignore-case</td><td>returns instances containing both "Ethernet" and "ethernet"</td></tr> </table>	show run grep Ethernet	returns a search result with instances containing a capitalized "Ethernet," such as <code>interface fortyGigE 0/0</code>	show run grep ethernet	does not return the previous search result because it only searches for instances containing a noncapitalized "ethernet"	show run grep Ethernet ignore-case	returns instances containing both "Ethernet" and "ethernet"
show run grep Ethernet	returns a search result with instances containing a capitalized "Ethernet," such as <code>interface fortyGigE 0/0</code>						
show run grep ethernet	does not return the previous search result because it only searches for instances containing a noncapitalized "ethernet"						
show run grep Ethernet ignore-case	returns instances containing both "Ethernet" and "ethernet"						
no-more	does not paginate the display output						
save	copies the output to a file for future use						

Displaying All Output

To display the output all at once (not one screen at a time), use the `no-more` option after the pipe. This operation is similar to the `terminal length screen-length` command except that the `no-more` option affects the output of just the specified command. For example: `Dell#show running-config | no-more`.

Filtering the Command Output Multiple Times

You can filter a single command output multiple times. To filter a command output multiple times, place the `save` option as the last filter. For example: `Dell# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save`.

Command Modes

To navigate and launch various CLI modes, use specific commands. Navigation to these modes is described in the following sections.

BGP ADDRESS-FAMILY Mode

To enable or configure IPv4 or IPv6 for BGP, use BGP ADDRESS-FAMILY mode. For more information, refer to [Border Gateway Protocol IPv4 \(BGPv4\)](#).

To enter BGP ADDRESS-FAMILY mode:

1. Verify that you are logged in to ROUTER BGP mode.
2. Enter the command `address-family` then the protocol type (`ipv4 multicast` or `ipv6 unicast`). The prompt changes to include (conf-router_bgp_af) for IPv4 or (conf-router_bgpv6_af) for IPv6.

CLASS-MAP Mode

To create or configure a class map, use CLASS-MAP mode. For more information, refer to [Policy-Based QoS Commands](#).

To enter CLASS-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `class-map` command then enter the class map name. The prompt changes to include (config-class-map).

You can return to CONFIGURATION mode by using the `exit` command.

CONFIGURATION Mode

In EXEC Privilege mode, use the `configure` command to enter CONFIGURATION mode and configure routing protocols and access interfaces.

To enter CONFIGURATION mode:

1. Verify that you are logged in to EXEC Privilege mode.
2. Enter the `configure` command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE mode by using the `interface` command.

CONTROL-PLANE Mode

To manage control-plane traffic, use CONTROL-PLANE mode. For more information, refer to [Control Plane Policing \(CoPP\)](#).

To enter CONTROL-PLANE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `control-plane-cpuqos` command. The prompt changes to include (conf-control-cpuqos).

You can return to CONFIGURATION mode by using the `exit` command.

DHCP Mode

To enable and configure Dynamic Host Configuration Protocol (DHCP), use DHCP mode. For more information, refer to [Dynamic Host Configuration Protocol \(DHCP\)](#).

To enter DHCP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip dhcp server` command. The prompt changes to include (config-dhcp).

You can return to CONFIGURATION mode by using the `exit` command.

DHCP POOL Mode

To create an address pool, use DHCP POOL mode. For more information, refer to [Dynamic Host Configuration Protocol \(DHCP\)](#).

To enter DHCP POOL mode:

1. Verify that you are logged in to DHCP mode.
2. Enter the `pool` command then the pool name. The prompt changes to include (config-dhcp-pool-name).

You can return to DHCP mode by using the `exit` command.

ECMP GROUP Mode

To enable or configure traffic distribution monitoring on an ECMP link bundle, use ECMP GROUP mode. For more information, refer to [ecmp_overview](#).

To enter ECMP GROUP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ecmp-group` command then enter the ECMP group ID. The prompt changes to include (conf-ecmp-group-ecmp-group-id).

You can return to CONFIGURATION mode by using the `exit` command.

EIS Mode

To enable or configure Egress Interface Selection (EIS), use EIS mode. For more information, refer to [EIS Commands](#).

To enter EIS mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `management egress-interface-selection` command. The prompt changes to include (conf-mgmt-eis).

You can return to CONFIGURATION mode by using the `exit` command.

EXEC Mode

When you initially log in to the switch, by default, you are logged in to EXEC mode. This mode allows you to view settings and enter EXEC Privilege mode, which is used to configure the device.

When you are in EXEC mode, the `>` prompt is displayed following the host name prompt, which is "Dell" by default. You can change the host name prompt using the `hostname` command.

 **NOTE:** Each mode prompt is preceded by the host name.

EXEC Privilege Mode

The `enable` command accesses EXEC Privilege mode. If an administrator has configured an "Enable" password, you are prompted to enter it.

EXEC Privilege mode allows you to access all the commands accessible in EXEC mode, plus other commands, such as to clear address resolution protocol (ARP) entries and IP addresses. In addition, you

can access CONFIGURATION mode to configure interfaces, routes and protocols on the switch. While you are logged in to EXEC Privilege mode, the # prompt is displayed.

EXTENDED COMMUNITY LIST Mode

To enable and configure a BGP extended community, use EXTENDED COMMUNITY LIST mode. For more information, refer to [BGP Extended Communities \(RFC 4360\)](#).

To enter EXTENDED COMMUNITY LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip extcommunity-list` command then a community list name. The prompt changes to include (conf-ext-community-list).

You can return to CONFIGURATION mode by using the `exit` command.

FRRP Mode

To enable or configure Force10 Resilient Ring Protocol (FRRP), use FRRP mode. For more information, refer to [Force10 Resilient Ring Protocol \(FRRP\)](#).

To enter FRRP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol frrp` command then the ring ID. The prompt changes to include (conf-frrp-ring-id).

You can return to CONFIGURATION mode by using the `exit` command.

GRUB Mode

To enable GRUB mode, press ESC when the following message appears during a system boot: `Press ESC key to stop autoreboot...` Select Force10 Boot using the arrow keys and then press the "C" key to enter the GRUB Command Line Interface. The command prompt changes to `grub>`.

INTERFACE Mode

Use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a 10-Gigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `interface` command and then enter an interface type and interface number that is available on the switch.

The prompt changes to include the designated interface and slot/port number. For example:

Prompt	Interface Type
Dell (conf-if) #	INTERFACE mode
Dell (conf-if-te-0/0) #	Ten-Gigabit Ethernet interface then slot/port information

Prompt	Interface Type
<code>Dell (conf-if-fo-0/0) #</code>	Forty-Gigabit Ethernet interface then slot/port information
<code>Dell (conf-if-lo-0) #</code>	Loopback interface number
<code>Dell (conf-if-nu-0) #</code>	Null Interface then zero
<code>Dell (conf-if-po-0) #</code>	Port-channel interface number
<code>Dell (conf-if-vl-0) #</code>	VLAN Interface then VLAN number (range 1–4094)
<code>Dell (conf-if-ma-0/0) #</code>	Management Ethernet interface then slot/port information
<code>Dell (conf-if-tu-0) #</code>	Tunnel interface then tunnel ID.
<code>Dell (conf-if-range) #</code>	Designated interface range (used for bulk configuration).

IP ACCESS LIST Mode

To enter IP ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `ip access-list standard` or `ip access-list extended` command.

To enter IP ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `ip access-list standard` or `ip access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-nacl) or (conf-ext-nacl).

You can return to CONFIGURATION mode by using the `exit` command.

LLDP Mode

To enable and configure Link Layer Discovery Protocol (LLDP), use LLDP mode. For more information, refer to [Link Layer Discovery Protocol \(LLDP\)](#).

To enter LLDP mode:

1. To enable LLDP globally, verify that you are logged in to CONFIGURATION mode. To enable LLDP on an interface, verify that you are logged in to INTERFACE mode.
2. Enter the `protocol lldp` command. The prompt changes to include (conf-lldp) or (conf-if-interface-lldp).

LLDP MANAGEMENT INTERFACE Mode

To enable and configure Link Layer Discovery Protocol (LLDP) on management interfaces, use LLDP MANAGEMENT INTERFACE mode. For more information, refer to the [Link Layer Discovery Protocol \(LLDP\)](#) chapter in the *Dell Networking Z9500 Configuration Guide*.

To enter LLDP MANAGEMENT INTERFACE mode:

1. Verify that you are logged in to LLDP mode.
2. Enter the `management-interface` command. The prompt changes to include (conf-lldp-mgmtlf).

LINE Mode

To configure the console or virtual terminal parameters, use LINE mode.

To enter LINE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `line` command. Include the keywords `console` or `vtty` and their line number available on the switch. The prompt changes to include (config-line-console) or (config-line-vty).

You can exit this mode by using the `exit` command.

MAC ACCESS LIST Mode

To enter MAC ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `mac access-list standard` or `mac access-list extended` command.

To enter MAC ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `mac access-list standard` or `mac access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-macl) or (conf-ext-macl).

You can return to CONFIGURATION mode by using the `exit` command.

MONITOR SESSION Mode

To enable and configure a traffic monitoring session using port monitoring, use MONITOR SESSION mode. For more information, refer to [Port Monitoring](#).

To enter MONITOR SESSION mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `monitor session` command then the session ID. The prompt changes to include (conf-mon-sess-sessionID).

MULTIPLE SPANNING TREE (MSTP) Mode

To enable and configure MSTP, use MULTIPLE SPANNING TREE mode. For more information, refer to [Multiple Spanning Tree Protocol \(MSTP\)](#).

To enter MULTIPLE SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree mstp` command. The prompt changes to include (conf-mstp).

You can return to CONFIGURATION mode by using the `exit` command.

Per-VLAN SPANNING TREE (PVST+) Plus Mode

To enable and configure the Per-VLAN Spanning Tree (PVST+) protocol, use PVST+ mode. For more information, refer to [Per-VLAN Spanning Tree Plus \(PVST+\)](#).



NOTE: The protocol name is PVST+, but the plus sign is dropped at the CLI prompt.

To enter PVST+ mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree pvst` command. The prompt changes to include (conf-pvst).

You can return to CONFIGURATION mode by using the `exit` command.

PORT-CHANNEL FAILOVER-GROUP Mode

To configure shared LAG state tracking, use PORT-CHANNEL FAILOVER-GROUP mode. For more information, refer to [Port Channel Commands](#).

To enter PORT-CHANNEL FAILOVER-GROUP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `port-channel failover-group` command. The prompt changes to include (conf-po-failover-grp).

You can return to CONFIGURATION mode by using the `exit` command.

PREFIX-LIST Mode

To configure a prefix list, use PREFIX-LIST mode.

To enter PREFIX-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip prefix-list` command. Include a name for the prefix list. The prompt changes to include (conf-nprefxl).

You can return to CONFIGURATION mode by using the `exit` command.

PRIORITY GROUP Mode

To create an ETS priority group, use PRIORITY GROUP mode.

To enter PRIORITY GROUP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `priority-group` command then the group name. The prompt changes to include (conf-pg).

You can return to CONFIGURATION mode by using the `exit` command.

PROTOCOL GVRP Mode

To enable and configure GARP VLAN Registration Protocol (GVRP), use PROTOCOL GVRP mode. For more information, refer to [GARP VLAN Registration \(GVRP\)](#).

To enter PROTOCOL GVRP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol gvrp` command. The prompt changes to include (config-gvrp).

You can return to CONFIGURATION mode by using the `exit` command.

QOS POLICY Mode

To configure ETS bandwidth allocation and scheduling for priority traffic, use QOS POLICY mode.

To enter QOS POLICY mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `qos-policy-output` command, then the policy name, then `ets`. The prompt changes to include (conf-qos-policy-out-ets).

You can return to CONFIGURATION mode by using the `exit` command.

RAPID SPANNING TREE (RSTP) Mode

To enable and configure RSTP, use RSTP mode. For more information, refer to [Rapid Spanning Tree Protocol \(RSTP\)](#).

To enter RSTP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree rstp` command. The prompt changes to include (conf-rstp).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTE-MAP Mode

To configure a route map, use ROUTE-MAP mode.

To enter ROUTE-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `route-map map-name [permit | deny] [sequence-number]` command. The prompt changes to include (config-route-map).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER BGP Mode

To enable and configure Border Gateway Protocol (BGP), use ROUTER BGP mode. For more information, refer to [Border Gateway Protocol IPv4 \(BGPv4\)](#).

To enter ROUTER BGP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `router bgp` command then enter the AS number. The prompt changes to include (conf-router_bgp).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER OSPF Mode

To configure OSPF, use ROUTER OSPF mode. For more information, refer to [Open Shortest Path First \(OSPFv2\)](#).

To enter ROUTER OSPF mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router ospf {process-id}` command. The prompt changes to include (conf-router_ospf-id).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER RIP mode by using the `router rip` command.

ROUTER OSPFV3 Mode

To configure OSPF for IPv6, use ROUTER OSPFV3 mode. For more information, refer to [Open Shortest Path First \(OSPFv2 and OSPFv3\)](#).

To enter ROUTER OSPFV3 mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ipv6 router ospf {process-id}` command. The prompt changes to include (conf-ipv6-router_ospf).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER RIP Mode

To enable and configure Router Information Protocol (RIP), use ROUTER RIP mode. For more information, refer to [Routing Information Protocol \(RIP\)](#).

To enter ROUTER RIP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `router rip` command. The prompt changes to include (conf-router_rip).

You can return to CONFIGURATION mode by using the `exit` command.

SPANNING TREE Mode

To enable and configure the Spanning Tree protocol, use SPANNING TREE mode. For more information, refer to [Spanning Tree Protocol \(STP\)](#).

To enter SPANNING TREE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree stp-id` command. The prompt changes to include (conf-stp).

You can return to CONFIGURATION mode by using the `exit` command.

TRACE-LIST Mode

To configure a Trace list, use TRACE-LIST mode.

To enter TRACE-LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip trace-list` command. Include the name of the Trace list. The prompt changes to include (conf-trace-acl).

You can exit this mode by using the `exit` command.

VRRP Mode

To enable and configure Virtual Router Redundancy Protocol (VRRP), use VRRP mode. For more information, refer to [Virtual Router Redundancy Protocol \(VRRP\)](#).

To enter VRRP mode:

1. To enable VRRP globally, verify that you are logged in to CONFIGURATION mode.
2. Enter the `vrrp-group` command then enter the VRRP group ID. The prompt changes to include *(conf-if-interface-type-slot/port-vrid-vrrp-group-id)*.

UPLINK STATE GROUP Mode

To enable and configure an uplink-state group, use UPLINK STATE GROUP mode. For more information, refer to [Uplink Failure Detection \(UFD\)](#).

To enter UPLINK STATE GROUP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `uplink-state-group` command then the group ID number. The prompt changes to include *(conf-uplink-state-group-groupID)*.

File Management

This chapter contains command line interface (CLI) commands needed to manage the configuration files as well as other file management commands.

The commands in this chapter are supported by the Dell Networking OS on the Z9500 switch.

boot system

Specify the location where the Dell Networking OS image used to boot the system is stored.

Z9500

Syntax

```
boot system {gateway ip address | {default | primary |
secondary} {system {A: | B:} | tftp: | ftp:}}
```

To return to the default boot sequence, use the `no boot system` command.

Parameters

gateway	Enter the IP address of the default next-hop gateway for the management subnet.
ip-address	Enter an IP address in dotted decimal format.
default	Enter the keyword <code>default</code> to use the default Dell Networking OS image.
primary	Enter the keyword <code>primary</code> to use the primary Dell Networking OS image.
secondary	Enter the keyword <code>secondary</code> to use the secondary Dell Networking OS image.
system A: B:	Enter <code>A:</code> or <code>B:</code> to boot one of the system partitions.
tftp:	Enter the keyword <code>TFTP:</code> to retrieve the image from a TFTP server: <code>tftp://host-ip/filepath</code> .
ftp:	Enter the keyword <code>FTP:</code> to retrieve the image from an FTP server: <code>ftp://userid:password@host-ip/filepath</code> .

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Usage Information

To display these changes in the `show bootvar` command output, save the running configuration to the startup configuration (using the `copy` command) and reload system.

format flash

Erase all existing files and reformat the file system in the internal flash memory or the USB drive. After the file system is formatted, files cannot be restored.

Z9500

Syntax

```
format [flash: | usbflash:]
```

Parameters

**flash: |
usbflash:**

- **flash:** reformat the file system in the internal flash memory.
- **usbflash:** reformat the file system in the USB flash drive.

Defaults

flash memory

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.

Usage Information

Include the colon (:) when entering this command.



CAUTION: This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the `write memory` command or `copy run start` command).

restore factory-defaults

Restore factory defaults on a switch.

Syntax	<code>restore factory-defaults {clear-all nvram}</code>	
Parameters	factory-defaults	Return the switch to its factory-default settings.
	clear-all	Enter the keywords <code>clear-all</code> to reset the NvRAM and the system startup configuration.
	nvram	Enter the keyword <code>nvram</code> to reset the NvRAM only.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.17.1	Supported on the M I/O Aggregator.
Usage Information	Restoring factory defaults deletes the existing startup configuration and all persistent settings (stacking, fanout, and so forth).	
	When restoring factory default settings, a switch remains in standalone mode after the restoration. After the restore is complete, the units power cycle immediately.	



CAUTION: There is no undo for this command.

Example

```
Dell# restore factory-defaults clear-all

*****
*****
* Warning - Restoring factory defaults will delete the
existing *
* startup-config and all persistent settings (stacking,
fanout, etc.)*
* After restoration the unit(s) will be powercycled
immediately.*
* Proceed with
caution !
*

*****
*****
```

Proceed with factory settings? Confirm [yes/no]:n

show boot system

Displays information about boot images currently stored on the system.

Z9500

Syntax	show boot system all		
Parameters	all	Display the boot images stored on the system for the Control Processor, Route Processor, and line card CPUs.	
Defaults	none		
Command Modes	- EXEC - EXEC Privilege		

Example

```
Dell#show boot system all

Current system image information in the system:
=====

Type           Boot Type      A              B
-----
CP              DOWNLOAD BOOT  9-3            9-3
RP              DOWNLOAD BOOT  9-3            9-3
linecard 0 is not present.
linecard 1 is not present.
linecard 2      DOWNLOAD BOOT  9-3            9-3
```

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

show bootvar

Display the variable settings for the boot parameters.

Z9500

Syntax show bootvar

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	Output expanded to display current reload mode (normal or Jumpstart).
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#show bootvar
PRIMARY IMAGE FILE = ftp://box:password@10.31.1.205//home/
5.3.1/5.3.1.0/FTOS-ZC-9.2.1.0.bin
SECONDARY IMAGE FILE = variable does not exist
DEFAULT IMAGE FILE = flash://FTOS-ZC-9.2.1.0.bin
LOCAL CONFIG FILE = variable does not exist
PRIMARY HOST CONFIG FILE = variable does not exist
SECONDARY HOST CONFIG FILE = variable does not exist
PRIMARY NETWORK CONFIG FILE = variable does not exist
SECONDARY NETWORK CONFIG FILE = variable does not exist
CURRENT IMAGE FILE = ftp://box:password@10.31.1.205//home/
5.3.1/5.3.1.0/FTOS-ZC-9.2.1.0.bin
CURRENT CONFIG FILE 1 = flash://startup-config
CURRENT CONFIG FILE 2 = variable does not exist
CONFIG LOAD PREFERENCE = local first
BOOT INTERFACE GATEWAY IP ADDRESS = variable does not exist
Dell#
```

Related Commands [boot system](#) — sets the location of Dell Networking OS image files.

show file

Display contents of a text file in the local filesystem.

Z9500

Syntax

Parameters

Command Modes

Command History

show file filesystem

filesystem

Enter one of the following:

- For internal flash, enter flash:
- For USB flash, enter usbflash:

EXEC Privilege

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series
E-Series	Original command

Example

```
Dell#show file flash://startup-config
!
boot system primary system ftp://test:server@10.16.1.144//home/
images/FTOS-ZC-9.2.1.0.bin
boot system secondary system flash://FTOS-ZC-9.2.1.0.bin
boot system default system ftp://:0/\
!
redundancy auto-synchronize persistent-data
redundancy primary rpm0
!
hostname Z9500-20
!
enable password 7 94849d8482d5c3
!
username test password 7 93e1e7e2ef
!
enable restricted 7 948a9d848cd5c3
!
protocol spanning-tree 0
bridge-priority 8192
rapid-root-failover enable
```

```

!
interface TenGigabitEthernet 0/0
no ip address
shutdown

```

**Related
Commands**

[format flash](#) — Erases all the existing files and reformats the file system in the internal flash memory.

show os-version

Display the release and software image version information of the image file specified.

Z9500

Syntax

```
show os-version [file-url]
```

Parameters

file-url

(OPTIONAL) Enter the following location keywords and information:

- For a file on the internal flash, enter `flash://` followed by the filename.
- For a file on an FTP server, enter `ftp://user:password@hostip/filepath`.
- For a file on the external Flash, enter `slot0://` followed by the filename.
- For a file on a TFTP server, enter `tftp://hostip/filepath`.
- For a file on the USB port, enter `usbflash://filepath`.

Defaults

none

**Command
Modes**

EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell# show os-version
```

RELEASE IMAGE INFORMATION :

```
-----
Platform      Version      Size      ReleaseTime
Z-Series:  ZC      9.2 (1.0B5)  99224598  Mar 15 2014
09:35:06
```

TARGET IMAGE INFORMATION :

```
-----
Type      Version      Target      checksum
runtime   9.2 (1.0B5)    CP          passed
runtime   9.2 (1.0B5)    LP          passed
runtime   9.2 (1.0B5)    RP          passed
```

BOOT IMAGE INFORMATION :

```
-----
Type      Version      Target      checksum
boot flash 3.2.1.0      cp          passed
```

BOOTSEL IMAGE INFORMATION :

```
-----
Type      Version      Target      checksum
boot selector 3.2.0.0      cp          passed
```

DEVICE IMAGE INFORMATION :

```
-----
Type      Version      Target
Portcard CPLD (0) 0xb5      LP (0)
Portcard CPLD (1) 0xb5      LP (0)
Portcard CPLD (2) 0xb5      LP (0)
Portcard CPLD (0) 0xb5      LP (1)
Portcard CPLD (1) 0xb5      LP (1)
Portcard CPLD (2) 0xb5      LP (1)
Portcard CPLD (3) 0xb5      LP (1)
Portcard CPLD (0) 0xb5      LP (2)
Portcard CPLD (1) 0xb5      LP (2)
Portcard CPLD (2) 0xb5      LP (2)
Portcard CPLD (3) 0xb5      LP (2)
System CPLD      0x0b      CP
FPGA            0x1c      CP
Backup FPGA      0x19      CP
```

Usage Information



NOTE: A filepath that contains a dot (.) is not supported.

show running-config

Display the current configuration and display changes from the default values.

Z9500

Syntax

```
show running-config [entity] [configured] [status]
```

Parameters

entity

(OPTIONAL) To display that entity's current (non-default) configuration, enter one of the following keywords:



NOTE: If you did not configure anything that entity, nothing displays and the prompt returns.

aaa	for the current AAA configuration
acl	for the current ACL configuration
arp	for the current static ARP configuration
as-path	for the current AS-path configuration
bfd	for the current BFD configuration
bgp	for the current BGP configuration
boot	for the current boot configuration
class-map	for the current class-map configuration
community-list	for the current community-list configuration
ecmp-group	for the current ECMP group configuration
eis	for the current EIS configuration
ethernet	for the current Ethernet CFM configuration
fe fd	for the current FEFD configuration
ftp	for the current FTP configuration
frrp	for the current FRRP configuration
fvrp	for the current FVRP configuration
gvrp	for the current GVRP configuration
host	for the current host configuration
hardware-monitor	for hardware-monitor action-on-error settings
hypervisor	for the current hypervisor configuration

igmp	for the current IGMP configuration
interface	for the current interface configuration
interface tunnel	for all configured tunnels. For a specific tunnel, enter the tunnel ID. The range is from 1 to 16383.
ip	for the current IP configuration
isis	for the current ISIS configuration
line	for the current line configuration
lldp	for the current LLDP configuration
load-balance	for the current port-channel load-balance configuration
logging	for the current logging configuration
mac	for the current MAC ACL configuration
mac-address- table	for the current MAC configuration
management- eis	for the current management EIS configuration
management- route	for the current Management port forwarding configuration
mld	for the current MLD configuration
monitor	for the current Monitor configuration
mroute	for the current Mroutes configuration
msdp	for the current MSDP configuration
ntp	for the current NTP configuration
ospf	for the current OSPF configuration
pim	for the current PIM configuration
policy-map- input	for the current input policy map configuration
policy-map- output	for the current output policy map configuration
po-failover- group	for the current port-channel failover-group configuration
prefix-list	for the current prefix-list configuration
privilege	for the current privilege configuration
qos-policy- input	for the current input QoS policy configuration

qos-policy-output	for the current output QoS policy configuration
radius	for the current RADIUS configuration
redirect-list	for the current redirect-list configuration
redundancy	for the current RPM redundancy configuration
resolve	for the current DNS configuration
rip	for the current RIP configuration
rmon	for the current RMON configuration
route-map	for the current route map configuration
sflow	for the current sFlow configuration
snmp	for the current SNMP configuration
spanning-tree	for the current spanning tree configuration
static	for the current static route configuration
status	for the file status information
tacacs+	for the current TACACS+ configuration
tftp	for the current TFTP configuration
trace-group	for the current trace-group configuration
trace-list	for the current trace-list configuration
uplink-state-group	for the uplink state group configuration
users	for the current users configuration
vlt	for the current VLT configuration
wred-profile	for the current wred-profile configuration

configured (OPTIONAL) Enter the keyword `configuration` to display line card interfaces with non-default configurations only.

status (OPTIONAL) Enter the keyword `status` to display the checksum for the running configuration and the start-up configuration.

Command Modes	EXEC Privilege														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Example	<pre> Dell#show running-config Current Configuration ... ! Version 9.2(1.0B2) ! Last configuration change at Thu Mar 6 02:10:35 2014 by default ! boot system primary system: A: boot system secondary system: A: boot system default system: A: boot system gateway 1.1.1.1 !... </pre>														
Example	<pre> Dell#show running-config status running-config checksum 0xB4B9BF03 startup-config checksum 0x8803620F Dell# </pre>														
Usage Information	The status option allows you to display the size and checksum of the running configuration and the startup configuration.														

show startup-config

Display the startup configuration.

Z9500

Syntax	<code>show startup-config</code>
Command Modes	EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on S-Series
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show startup-config
! Version 9.2(1.0B2)
! Last configuration change at Mon Feb  3 11:24:00 2014 by
default
! Startup-config last updated at Mon Feb  3 11:24:05 2014 by
default
!
boot system primary system: A:
boot system secondary system: A:
boot system default system: A:
boot system gateway 1.1.1.1
!
...
```

Related Commands

[show running-config](#) – displays the current (running) configuration.

show version

Display the current Dell Networking OS version information on the system.

Z9500

Syntax

show version

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 9.2(1.0B5)
Copyright (c) 1999-2013 by Dell Inc. All Rights Reserved.
Build Time: Sat Mar 15 09:02:21 PDT 2014
Build Path: /work.local/build/toolSpaces/tools05/E9-2-1/SW/SRC
Force10 uptime is 15 minute(s)

System image file is "pt-z9500-5"

System Type: Z9500
Control Processor: Intel Centerton with 3 Gbytes (3203928064
bytes) of memory, cores(s) 1.

16G bytes of boot flash memory.

  1 36-port TE/FG (ZC)
  2 48-port TE/FG (ZC)
520 Ten GigabitEthernet/IEEE 802.3 interface(s)
  2 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

Command Fields

Lines Beginning With	Description
Dell Force10 Network...	Name of the operating system
Dell Force10 Operating...	OS version number
Dell Force10 Application...	Software version
Copyright (c)...	Copyright information
Build Time...	Software build's date stamp
Build Path...	Location of the software build files loaded on the system
Dell Force10 uptime is...	Amount of time the system has been up
System image...	Image file name

Lines Beginning With	Description
Chassis Type:	Chassis type (for example, E1200, E600, E600i, E300, C300, C150, S25, S50, S55, S60, S4810)
Control Processor:...	Control processor information and amount of memory on processor
Route Processor 1:...	Route processor 1 information and the amount of memory on that processor
Route Processor 2:...	Route processor 2 information and the amount of memory on that processor
128K bytes...	Amount and type of memory on system
1 Route Processor...	Hardware configuration of the system, including the number and type of physical interfaces available

Example

```
Dell#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 9.2(1.0B5)
Copyright (c) 1999-2013 by Dell Inc. All Rights Reserved.
Build Time: Sat Mar 15 09:02:21 PDT 2014
Build Path: /work.local/build/toolSpaces/tools05/E9-2-1/SW/SRC
Force10 uptime is 15 minute(s)

System image file is "pt-z9500-5"

System Type: Z9500
Control Processor: Intel Centerton with 3 Gbytes (3203928064
bytes) of memory, cores(s) 1.

16G bytes of boot flash memory.

  1 36-port TE/FG (ZC)
  2 48-port TE/FG (ZC)
520 Ten GigabitEthernet/IEEE 802.3 interface(s)
  2 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

upgrade boot

Upgrade the bootflash or bootselector image running in all Z9500 CPUs, including the Control Processor, Route Processor, and line cards. To upgrade the operating system image, use the `upgrade system` command.

Z9500

Syntax

```
upgrade boot {bootflash-image | bootselector-image} system all
{booted | flash: | ftp: | scp: | tftp: | usbflash:} file-url
{A: |B:}
```

Parameters

bootflash-image	Enter the keyword <code>bootflash-image</code> to upgrade the GRUB bootloader image.
bootselector-image	Enter the keyword <code>bootselector-image</code> to upgrade the BIOS system image. Use this option only with TAC supervision.
system all	Enter the keywords <code>system all</code> to upgrade the bootflash or bootselector image on all Z9500 CPUs: Control Processor, Route Processor, and line-card CPUs.
booted	Enter the keyword <code>booted</code> to upgrade Z9500 CPUs using the currently loaded operating system (OS) image.
flash: ftp: scp: tftp: usbflash: file-url	Enter one of the file transfer methods and locations to specify where the OS image (<i>file-url</i>), which you want to use to upgrade the currently loaded image, is stored: <code>flash://filepath.</code> <code>ftp://userid:password@host-ip/filepath</code> to upgrade from an FTP server, where <i>host-ip</i> is either an IPv4 dotted decimal address or an IPv6 [x:x:x::x] format address. <code>scp://userid:password@hostip/filepath</code> to upgrade using secure copy. <code>tftp://host-ip/filepath</code> to upgrade from a TFTP server, where <i>host-ip</i> is either an IPv4 dotted decimal address or an IPv6 [x:x:x::x] format address. <code>usbflash://filepath</code> to upgrade form an external flash device.
A: B:	Specify the boot-flash partition to be upgraded.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0(0.0)	Added support for IPv6 for the <i>file-url</i> parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.
8.3.7.0	Introduced on the S4810.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.7.1.0</td><td>Added support for TFTP and SCP.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	7.7.1.0	Added support for TFTP and SCP.	7.6.1.0	Introduced on the S-Series.
Version	Description						
7.7.1.0	Added support for TFTP and SCP.						
7.6.1.0	Introduced on the S-Series.						
Usage Information	A system message displays with status information about the bootflash upgrade. RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [X:X:X:X::X]. For maximum flexibility this command accepts IPv6 host addresses with or without the square brackets. Reload the system after executing this command.						
Example	<pre> Dell# upgrade boot all system all booted Current Boot information in the system: ===== Card BootFlash Current Version New Version ----- Linecard0 Boot Flash 3.2.1.0 3.2.1.0 Linecard1 Boot Flash 3.2.1.0 3.2.1.0 Linecard2 Boot Flash 3.2.1.0 3.2.1.0 ***** * Warning - Upgrading boot flash is inherently risky and should only * * be attempted when necessary. A failure at this upgrade may cause * * a board RMA. Proceed with caution ! * ***** Dell# </pre>						

upgrade fpga-image linecard booted

Use this command to upgrade the FPGA and CPLD devices in Z9500 line-card CPUs using the currently running Dell Networking operating-system image (and only when required by the upgrade procedure in the Z9500 release notes).

Z9500

Syntax	upgrade fpga-image linecard { <i>slot-id</i> all} booted	
Parameters	linecard <i>slot-id</i>	Enter the slot ID number to specify the line-card CPU to upgrade. The range of Z9500 slot IDs is 0 to 2. Enter linecard all to upgrade all Z9500 line cards.
Defaults	none	

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z-Series.

Example

```
Dell# upgrade fpga-image linecard all booted

Current FPGA information in the system:
=====

Card          FPGA Name      Current Version  New Version
-----
Linecard0     PORTCARD CPLD   0xac             0xb2
Linecard1     PORTCARD CPLD   0xab             0xb2

*****
*****
* Warning - Upgrading FPGA is inherently risky and should      *
* only be attempted when necessary. A failure at this upgrade  *
* may cause a board RMA. Proceed with caution !                *
*****
*****

*****
*****
* When the upgrade has successfully completed, the system will *
* be automatically rebooted to reload the upgraded             *
* components.                                                   *
*****
*****

Upgrade CPLD image for system [yes/no]: yes

FPGA upgrade in progress!!! Please do NOT power off the unit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Usage Information

Do not restart the switch while an upgrade is progressing. Restarting the chassis during an upgrade may corrupt critical boot components.

When an upgrade of FPGA devices successfully completes, the switch reloads automatically.

Related Commands

- [upgrade fpga-image system fpga booted](#) — upgrades the FPGA devices in all Z9500 CPUs.

upgrade fpga-image system cpld booted

Use this command to upgrade the CPLD devices in the Z9500 Route Processor and Control Processor CPUs using the currently running Dell Networking operating-system image (and only when required by the upgrade procedure in the Z9500 release notes).

Z9500

Syntax upgrade fpga-image system cpld booted

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z-Series.
8.3.1.0	Added the rpm option.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell# upgrade fpga-image system cpld booted
```

```
Current information in the system:
=====
```

Card	FPGA Name	Current Version	New Version
CP	SYSTEM CPLD	0x07	0x08

```
*****
* Warning - Upgrading FPGA is inherently risky and should      *
* only be attempted when necessary. A failure at this upgrade  *
* may *
* cause a board RMA. Proceed with caution !                    *
*****

*****
* When the upgrade has successfully completed, the system will *
* be *
* automatically rebooted to reload the upgraded                *
components. *
*****
```

```
*****

Upgrade CPLD image for system [yes/no]: yes

FPGA upgrade in progress!!! Please do NOT power off the unit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Usage Information

Do not restart the switch while an upgrade is progressing. Restarting the chassis during an upgrade may corrupt critical boot components.

When an upgrade of CPLD devices successfully completes, the switch reloads automatically.

Related Commands

- [upgrade fpga-image system fpga](#) — upgrades the CPLD devices in all Z9500 CPUs.

upgrade fpga-image system fpga booted

Use this command to upgrade the FPGA devices in the Z9500 Route Processor and Control Processor CPUs using the currently running Dell Networking operating-system image (and only when required by the upgrade procedure in the Z9500 release notes).

Z9500

Syntax

```
upgrade fpga-image system fpga booted
```

Defaults

```
none
```

Command Modes

```
EXEC Privilege
```

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z-Series.

Example

```
Dell# upgrade fpga-image system fpga booted
```

```
Current FPGA information in the system:
=====
```

Card	FPGA Name	Current Version	New Version
-----	-----	-----	-----
CP	FPGA	0x14	0x13

```

*****
*****
* Warning - Upgrading FPGA is inherently risky and should      *
* only be attempted when necessary. A failure at this upgrade  *
may      *
* cause a board RMA. Proceed with caution !      *
*****
*****

Upgrade FPGA image for system [yes/no]: yes

FPGA upgrade in progress!!! Please do NOT power off the unit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

Usage Information

Do not restart the switch while an upgrade is progressing. Restarting the chassis during an upgrade may corrupt critical boot components.

When an upgrade of FPGA devices successfully completes, the switch reloads automatically.

Related Commands

- [upgrade fpga-image linecard booted](#) — upgrades the FPGA devices in Z9500 line cards.

upgrade system

Upgrade the Dell Networking OS image on all Z9500 CPUs, including the Control Processor, Route Processor, and line cards. To upgrade the bootflash or bootselector image, use the `upgrade boot` command.

Z9500

Syntax

```
upgrade system {ftp: | scp: | tftp: | flash: | usbflash:} file-
url {A: |B:}
```

Parameters

system	Enter the keyword <code>system</code> to upgrade the operating system (OS) image.
ftp: file-url	Enter the keyword <code>ftp:</code> and specify the location of the image file in the format <code>//userid:password@host-ip/filepath</code> or press Enter to launch a prompt sequence.
scp: file-url	Enter the keyword <code>scp:</code> and specify the location of the image file in the format <code>userid:password@host-ip/filepath</code> or press Enter to launch a prompt sequence.

	tftp: <i>file-url</i> Enter the keyword <code>tftp:</code> and specify the location of the image file in the format <code>//host-ip/filepath</code> or press Enter to launch a prompt sequence. flash: <i>file-url</i> Enter the keyword <code>flash:</code> and specify the location of the image file in the format <code>//directory-path</code> or press Enter to launch a prompt sequence. usbflash: <i>file-url</i> Enter the keyword <code>usbflash:</code> and specify the location of the source file in the format <code>//directory-path</code> to upgrade from an external flash device or press Enter to launch a prompt sequence. A: B: Specify the flash partition of the operating-system image to be upgraded.																
Defaults	none																
Command Modes	EXEC Privilege																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0(0.0)</td><td>Added support for IPv6 for the <code>file-url</code> parameter.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000. Added support for the SSD on the Z9000 only.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Added support for TFTP and SCP.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.0(0.0)	Added support for IPv6 for the <code>file-url</code> parameter.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Added support for TFTP and SCP.	7.6.1.0	Introduced on the S-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
9.0(0.0)	Added support for IPv6 for the <code>file-url</code> parameter.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.																
8.3.7.0	Introduced on the S4810.																
7.7.1.0	Added support for TFTP and SCP.																
7.6.1.0	Introduced on the S-Series.																
Usage Information	RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [X:X:X:X:X]. For maximum flexibility this command accepts IPv6 host addresses with or without the square brackets. After you upgrade the system image, by entering the command, specify the location where the Dell Networking OS image used to boot the system is stored (<code>boot system</code>), save the configuration to the start-up config file (<code>write memory</code>), and reload the system (<code>reload</code>).																
Example	<pre>Dell# upgrade system tftp://10.11.8.12/dv-rainier-13 a: 00:39:32 : Discarded 1 pkts. Expected block num : 51. Received block num: 50 !00:39:36 : Discarded 1 pkts. Expected block num : 65. Received block num: 64</pre>																

verify

Syntax	<code>verify { md5 sha256 } [flash://] img-file [hash-value]</code>	
Parameters	md5	Enter the <code>md5</code> keyword to use the MD5 message-digest algorithm.
	sha256	Enter the <code>sha256</code> keyword to use the SHA256 Secure Hash Algorithm
	flash://	(Optional). Enter the <code>flash://</code> keyword. The default is to use the flash drive. You can just enter the image file name.
	img-file	Enter the name the Dell Networking software image file to validate.
	hash-value	(Optional). Enter the relevant hash published on i-Support.
Default	flash drive	
Command Modes	EXEC mode	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	You can enter this command in the following ways: verify md5 flash://img-file	

- **verify md5 flash:***//img-file <hash-value>*
- **verify sha256 flash:***//img-file*
- **verify sha256 flash:***//img-file <hash-value>*

Example

Without Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
SHA256 hash for FTOS-SE-9.5.0.0.bin:
e6328c06faf814e6899ceed219afbf9360e986d692988023b749e6b2093e93
3
```

Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
e6328c06faf814e6899ceed219afbf9360e986d692988023b749e6b2093e93
3
SHA256 hash VERIFIED for FTOS-SE-9.5.0.0.bin
```

Control and Monitoring

This chapter contains the commands to configure and monitor the system, including Telnet, file transfer protocol (FTP), and trivial file transfer protocol (TFTP) as they are implemented in the Dell Networking OS on the Z9500 switch.

asf-mode

Enable the transmission of Alternate Store and Forward (ASF) packets as soon as a threshold is reached.

Z9500

Syntax	<code>asf-mode linecard {slot-id all}</code> To return to standard Store and Forward mode, use the <code>no asf-mode linecard</code> command.											
Parameters	linecard slot-id	Enter the slot ID of a Z9500 line card. The range of slot IDs is from 0 to 2. Enter <code>all</code> to enable ASF mode on all line cards on the switch.										
Defaults	Not configured											
Command Modes	CONFIGURATION											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.0	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.19.0	Introduced on the S4820T.											
8.3.11.0	Introduced on the Z9000.											
8.3.7.0	Introduced on the S4810.											
Usage Information	You <i>must</i> save the configuration and reload the system to implement ASF. When you enter the command, the system sends a message stating that the new mode is enabled when the system reloads.											

banner exec

Configure a message that is displayed when your enter EXEC mode.

Z9500

Syntax	<code>banner exec c line c</code> To delete a banner, use the <code>no banner exec</code> command.	
Parameters	c	Enter the keywords <code>banner exec</code> , then enter a character delineator, represented here by the letter <code>c</code> . Press ENTER .
	line	Enter a text string for your banner message ending the message with your delineator. In the following example, the delineator is a percent character (%); the banner message is "testing, testing".
Defaults	No banner is displayed.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original Command

Usage Information	After entering the <code>banner exec</code> command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When you connect to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After logged in, the EXEC banner (if configured) displays.
Example	<pre>Dell(conf)#banner exec ? LINE c banner-text c, where 'c' is a delimiting character Dell(conf)#banner exec % Enter TEXT message. End with the character '%'. This is the banner%</pre>


```

Dell(conf)#end
Dell#exit
4d21h5m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated
for user on line
console

This is the banner

FTOS con0 now available

Press RETURN to get started.
4d21h6m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful for
user on line
console
This is the banner
Dell>

```

**Related
Commands**

[exec-banner](#) — Enables the display of a text string when you enter EXEC mode.

[line](#) — enables and configures the console and virtual terminal lines to the system.

banner login

Set a banner to display when logging on to the system.

Z9500

Syntax `banner login {keyboard-interactive | no keyboard-interactive}
[c line c]`

Parameters

keyboard-interactive	Enter the keyword <code>keyboard-interactive</code> to require a carriage return (CR) to get the message banner prompt.
c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
line	Enter a text string for your text banner message ending the message with your delineator. The delineator is a percent character (%). Range: maximum of 50 lines, up to 255 characters per line

Defaults No banner is configured and the CR is required when creating a banner.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced the keyword <code>keyboard-interactive</code> .
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Usage Information

After entering the banner login command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When the user is connected to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After the user has logged in, the EXEC banner (if configured) displays.

Example

```
Dell(conf)#banner login ?
keyboard-interactive Press enter key to get prompt
LINE c banner-text c, where 'c' is a delimiting character
Dell(conf)#no banner login ?
keyboard-interactive Prompt will be displayed by default
<cr>
Dell(conf)#banner login keyboard-interactive

Enter TEXT message. End with the character '%'.
This is the banner%
Dell(conf)#end
Dell#exit

13d21h9m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated
for user on line console

This is the banner

FTOS con0 now available

Press RETURN to get started.
13d21h10m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful
for user on line console
This is the banner
Dell>
```

Related Commands

[banner motd](#) — sets a Message of the Day banner.

[exec-banner](#) — enables the display of a text string when you enter EXEC mode.

banner motd

Set a message of the day (MOTD) banner.

Z9500

Syntax	banner motd <i>c line c</i>																			
Parameters	c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).																		
	line	Enter a text string for your MOTD banner the message with your delineator. The delineator is a percent character (%).																		
Defaults	No banner is configured.																			
Command Modes	CONFIGURATION																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>E-Series</td><td>Original command</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.12.0	Introduced on the S4810.																			
8.3.11.1	Introduced on the Z9000.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
E-Series	Original command																			
Usage Information	After entering the banner login command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When the user is connected to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After the user has logged in, the EXEC banner (if configured) displays.																			
Related Commands	banner exec — enables the display of a text string when you enter EXEC mode.																			
	banner login — sets a banner to display after successful login to the system.																			

cam-acl

Allocate content addressable memory (CAM) for IPv4 and IPv6 ACLs.

Z9500

Syntax `cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos number l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos] number ecfmacl number {openflow {4|8}}`

Parameters

default	Use the default CAM profile settings and set the CAM as follows: • L3 ACL (ipv4acl): 4 • L2 ACL(l2acl): 6 • IPv6 L3 ACL (ipv6acl): 0 • L3 QoS (ipv4qos): 2 • L2 QoS (l2qos): 1 • OpenFlow: 0 (disabled) • FCoE (fcoeacl): 0 (disabled) • iSCSI Optimization (iscsiptacl): 0 (disabled)
l2acl <i>number</i>	Allocate space to each CAM region.
ipv4acl <i>number</i>	
ipv6acl <i>number</i>	Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The ipv6acl range must be a factor of 2.
ipv4qos	
<i>number</i> l2qos	
<i>number</i> l2pt	Enter 4 or 8 for the number of OpenFlow FP blocks.
<i>number</i>	
ipmacacl	
<i>number</i> [vman-qos vman-dual-qos]	• 4: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality) • 8: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality)
<i>number</i>	
ecfmacl	
<i>number</i>	
{openflow {4 8}}	

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.2(0.0)	Added support for the <code>fcoe</code> parameter on the S4810 and S4820T.
9.1(0.0)	Added support for OpenFlow on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added the keywords <code>fcoeacl</code> and <code>iscsiopacl</code> on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Added the keywords <code>ecfmacl</code> , <code>vman-qos</code> , and <code>vman-dual-qos</code> .
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information	For the new settings to take effect, save the new CAM settings to the startup-config (<code>write-mem</code> or <code>copy run start</code>) then reload the system. The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated. The <code>ipv4acl</code> profile range is from 1 to 4. When configuring space for IPv6 ACLs, the total number of Blocks must equal 13. Ranges for the CAM profiles are from 1 to 10, except for the <code>ipv6acl</code> profile which is from 0 to 10. The <code>ipv6acl</code> allocation must be a factor of 2 (2, 4, 6, 8, 10). If you enabled BMP 3.0, to perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, use the <code>reload conditional nvram-cfg-change</code> command.
--------------------------	---

cam-audit linecard

Enable audit of the IPv4 forwarding table on all line cards.

Z9500

Syntax	<code>cam-audit linecard all ipv4-fib interval <i>time-in-minutes</i></code>	
Parameters	all	Enter the keyword <code>all</code> to enable CAM audit on all line cards.
	ipv4-fib	Enter the keyword <code>ipv4-fib</code> to designate the CAM audit on the IPv4 forwarding entries.

	interval time-in-minutes	Enter the keyword <code>interval</code> followed by the frequency in minutes of the CAM audit. Range: 5 to 1440 minutes (24 hours). Default: 60 minutes .
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced on the E-Series.
Usage Information	Enables periodic audits of the software and hardware copies of the IPv4 forwarding table.	

clear alarms

Clear alarms on the system.

Z9500

Syntax	<code>clear alarms</code>																		
Command Modes	EXEC Privilege																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>E-Series</td><td>Original command.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.12.0	Introduced on the S4810.																		
8.3.11.1	Introduced on the Z9000.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
E-Series	Original command.																		

**Usage
Information**

This command clears alarms that are no longer active. If an alarm situation is still active, it is seen in the system output.

clear line

Reset a terminal line.

Z9500

Syntax

```
clear line {line-number | console 0 | vtty number}
```

Parameters

<i>line-number</i>	Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
console 0	Enter the keywords <code>console 0</code> to reset the console port.
<i>vtty number</i>	Enter the keyword <code>vtty</code> then a number to clear a terminal line. The range is from 0 to 9.

**Command
Modes**

EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

clear trace

Clear the software trace log file from a Z9500 CPU.

Z9500

Syntax	<code>clear trace software [rp linecard slot-id]</code>	
Parameters	rp	Enter the keyword <code>rp</code> to clear the software trace log from the Route Processor CPU.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify the line-card CPU whose software trace log you want to clear.
Defaults	Clear the trace log files from all Z9500 CPUs.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.5.1.0	Introduced on the C-Series.
Usage Information	Trace log information is uploaded to <code>flash:/TRACE_LOG_DIR</code> .	

configure

Enter CONFIGURATION mode from EXEC Privilege mode.

Z9500

Syntax	<code>configure [terminal]</code>	
Parameters	terminal	(OPTIONAL) Enter the keyword <code>terminal</code> to specify that you are configuring from the terminal.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#configure
Dell(conf)#
```

debug cpu-traffic-stats

Enable the collection of computer processor unit (CPU) traffic statistics.

Z9500

Syntax

```
debug cpu-traffic-stats
```

To disable the debugging, use the `no debug cpu-traffic-stats` command.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	6.2.1.1	Introduced on the E-Series.
Version	Description				
6.2.1.1	Introduced on the E-Series.				
Usage Information	This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic a CPU receives automatically triggers (turn on) the collection of CPU traffic statics. The following message is an indication that collection of CPU traffic is automatically turned on. To view the traffic statistics, use the <code>show cpu-traffic-stats</code> command. If the CPU receives excessive traffic, traffic is rate controlled.  NOTE: This command must be enabled before the <code>show cpu-traffic-stats</code> command displays traffic statistics. Dell Networking recommends disabling debugging (<code>no debug cpu-traffic-stats</code>) after troubleshooting is complete.				
Related Commands	show cpu-traffic-stats — displays the cpu traffic statistics.				

debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server.

Z9500

Syntax	<code>debug ftpserver</code>
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

disable

Return to EXEC mode.

Z9500

Syntax	<code>disable [level]</code>	
Parameters	<i>level</i>	(OPTIONAL) Enter a number for a privilege level of the Dell Networking OS. The range is from 0 to 15. The default is 1 .
Defaults	1	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

do

Allows the execution of most EXEC-level commands from all CONFIGURATION levels without returning to the EXEC level.

Z9500

Syntax	do <i>command</i>																			
Parameters	<i>command</i>	Enter an EXEC-level command.																		
Defaults	none																			
Command Modes	• CONFIGURATION • INTERFACE																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.12.0	Introduced on the S4810.																			
8.3.11.1	Introduced on the Z9000.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.0	Introduced on the E-Series.																			
Usage Information	The following commands are <i>not</i> supported by the do command: • enable • disable • exit • config																			
Example	<pre>Dell(conf-if-te-5/0)#do clear counters Clear counters on all interfaces [confirm] Dell(conf-if-te-5/0)# Dell(conf-if-te-5/0)#do clear logging Clear logging buffer [confirm] Dell(conf-if-te-5/0)# Dell(conf-if-te-5/0)#do reload System configuration has been modified. Save? [yes/no]: n</pre>																			

```
Proceed with reload [confirm yes/no]: n
Dell(conf-if-te-5/0) #
```

enable

Enter EXEC Privilege mode or any other privilege level configured. After entering this command, you may need to enter a password.

Z9500

Syntax	enable [level]	
Parameters	level	(OPTIONAL) Enter a number for a privilege level of Dell Networking OS. The range is from 0 to 15.
Defaults	15	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information	Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the enable password command to configure a password for the enable command
-------------------	--

at a specific privilege level. If no privilege level is specified, the default is privilege level **15**.



NOTE: If you are authorized for the EXEC Privilege mode by your role, you do not need to enter an enable password.

**Related
Commands**

[enable password](#) — configures a password for the `enable` command and to access a privilege level.

enable optic-info-update interval

Enable polling intervals of optical information updates for simple network management protocol (SNMP).

Z9500

Syntax

`enable optical-info-update interval seconds`

To disable optical power information updates, use the `no enable optical-info-update interval` command.

Parameters

**interval
*seconds***

Enter the keyword `interval` then the polling interval in seconds. The range is from 120 to 6000 seconds. The default is **300 seconds** (5 minutes).

Defaults

Disabled

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Replacement command for the S4820T. Replaces the <code>enable xfp-power-updates</code> command.
8.3.11.4	Replacement command for the Z9000. Replaces the <code>enable xfp-power-updates</code> command
8.3.10.0	Replacement command for the S4810 only. Replaces the <code>enable xfp-power-updates</code> command.

**Usage
Information**

To enable polling and to configure the polling frequency, use this command.

end

Return to EXEC Privilege mode from other command modes (for example, CONFIGURATION or ROUTER OSPF modes).

Z9500

Syntax	end
Command Modes	• CONFIGURATION • SPANNING TREE • MULTIPLE SPANNING TREE • LINE • INTERFACE • TRACE-LIST • VRRP • ACCESS-LIST • PREFIX-LIST • AS-PATH ACL • COMMUNITY-LIST • ROUTER OSPF • ROUTER RIP • ROUTER ISIS • ROUTER BGP

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.
E-Series	Original command.

Related Commands	exit — returns to the lower command mode.
------------------	---

exec-banner

Enable the display of a text string when the user enters EXEC mode.

Z9500

Syntax	<code>exec-banner</code> To disable the banner on terminal lines, use the <code>no exec-banner</code> command.																		
Defaults	Enabled on all lines (if configured, the banner appears).																		
Command Modes	LINE																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>E-Series</td><td>Original command.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.7.0	Introduced on the S4810.																		
8.3.11.1	Introduced on the Z9000.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
E-Series	Original command.																		
Usage Information	Optionally, use the <code>banner exec</code> command to create a text string that is displayed when you access EXEC mode. This command toggles that display.																		
Related Commands	banner exec — configures a banner to display when entering EXEC mode. line — enables and configures console and virtual terminal lines to the system.																		

exec-timeout

Set a time interval that the system waits for input on a line before disconnecting the session.

Z9500

Syntax	<code>exec-timeout <i>minutes</i> [<i>seconds</i>]</code>
--------	---

To return to default settings, use the `no exec-timeout` command.

Parameters	minutes Enter the number of minutes of inactivity on the system before disconnecting the current session. The range is from 0 to 35791. The default is 10 minutes for the console line and 30 minutes for the VTY line. seconds (OPTIONAL) Enter the number of seconds. The range is from 0 to 2147483. The default is 0 seconds.																
Defaults	10 minutes for console line; 30 minutes for VTY lines; 0 seconds																
Command Modes	LINE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>E-Series</td><td>Original command.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Introduced on the S4810.																
8.3.11.1	Introduced on the Z9000.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
E-Series	Original command.																
Usage Information	To remove the time interval, enter <code>exec-timeout 0 0</code> .																
Example	<pre>FTOS con0 is now available Press RETURN to get started. Dell></pre>																

exit

Return to the lower command mode.

Z9500

Syntax	<code>exit</code>
--------	-------------------

Command Modes

- EXEC Privilege
- CONFIGURATION
- LINE, INTERFACE
- TRACE-LIST
- PROTOCOL GVRP
- SPANNING TREE
- MULTIPLE SPANNING TREE
- MAC ACCESS LIST
- ACCESS-LIST
- AS-PATH ACL
- COMMUNITY-LIST
- PREFIX-LIST
- ROUTER OSPF
- ROUTER RIP
- ROUTER ISIS
- ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Related Commands

[end](#) — returns to EXEC Privilege mode.

ftp-server enable

Enable FTP server functions on the system.

Z9500

Syntax ftp-server enable

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 FTOS (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size  date          time name
-----  -
512  Jul-20-2004  18:15:00 tgting
512  Jul-20-2004  18:15:00 diagnostic
512  Jul-20-2004  18:15:00 other
512  Jul-20-2004  18:15:00 tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Related
Commands

[ftp-server topdir](#) — sets the directory to be used for incoming FTP connections to the E-Series.

[ftp-server username](#) — sets a username and password for incoming FTP connections to the E-Series.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

Z9500

Syntax `ftp-server topdir directory`

Parameters

<i>directory</i>	Enter the directory path.
-------------------------	---------------------------

Defaults The internal flash is the default directory.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information After you enable FTP server functions with the `ftp-server enable` command, Dell Networking recommends specifying a top-level directory path. Without a top-level directory path specified, the system directs users to the flash directory when logging in to the FTP server.

Related Commands [ftp-server enable](#) — enables FTP server functions on the switch.

[ftp-server username](#) — sets a username and password for incoming FTP connections.

ftp-server username

Create a user name and associated password for incoming FTP server sessions.

Z9500

Syntax

```
ftp-server username username password [encryption-type]  
password
```

To delete a user name and its password, use the `no ftp-server username username` command.

Parameters

<i>username</i>	Enter a text string up to 40 characters long as the user name.
<i>password</i> <i>password</i>	Enter the keyword <code>password</code> then a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
<i>encryption-type</i>	(OPTIONAL) After the keyword <code>password</code> , enter one of the following numbers: • 0 (zero) for an unencrypted (clear text) password • 7 (seven) for a hidden text password

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

hostname

Set the host name of the system.

Z9500

Syntax `hostname name`

Parameters

<i>name</i>	Enter a text string, up to 32 characters long.
--------------------	--

Defaults **Dell**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Changed the default from Force10 to FTOS.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information The host name is used in the command-line prompt.

ip ftp password

Specify a password for outgoing FTP connections.

Z9500

Syntax `ip ftp password [encryption-type] password`
To remove a password and return to the default setting, use the `no ip ftp password [password]` command.

Parameters	<i>encryption-type</i>	(OPTIONAL) Enter one of the following numbers: • 0 (zero) for an unencrypted (clear text) password • 7 (seven) for a hidden text password
	<i>password</i>	Enter a string up to 40 characters as the password.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information	The password is listed in the configuration file; you can view the password by entering the <code>show running-config ftp</code> command. Use the <code>ip ftp password</code> command when you use the <code>ftp:</code> parameter in the <code>copy</code> command.
Related Commands	ip ftp username — sets the user name for the FTP sessions.

ip ftp source-interface

Configure an interface's IP address as the source IP address for FTP connections.

Z9500

Syntax `ip ftp source-interface interface`
To delete an interface, use the `no ip ftp source-interface interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a tunnel interface, enter the keyword <code>tunnel</code>.
------------------	---

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

ip ftp username

Assign a user name for outgoing FTP connection requests.

Z9500

Syntax	<pre>ip ftp username <i>username</i></pre> To return to anonymous FTP connections, use the <code>no ip ftp username [<i>username</i>]</code> command.																		
Parameters	<i>username</i> Enter a text string as the user name up to 40 characters long.																		
Defaults	No user name is configured.																		
Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>E-Series</td><td>Original command.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.12.0	Introduced on the S4810.																		
8.3.11.1	Introduced on the Z9000.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
E-Series	Original command.																		
Usage Information	Configure a password with the <code>ip ftp password</code> command.																		

ip http source-interface

Configure an interface's IP address as the source IP address for HTTP connections.

Z9500

Syntax

```
ip http source-interface interface
```

To delete an interface, use the `no ip http source-interface interface` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Defaults

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes

CONFIGURATION

Command History

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.3.11.1	Introduced on the Z9000
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094)
8.1.1.0	Introduced on E-Series ExaScale
7.6.1.0	Support added for S-Series

Version	Description
7.5.1.0	Introduced on C-Series

ip telnet server enable

Enable the Telnet server on the switch.

Z9500

Syntax	<pre>ip telnet server enable</pre> To disable the Telnet server, use the <code>no ip telnet server enable</code> command.														
Defaults	Enabled														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.11.1	Introduced on the Z9000.														
8.1.1.0	Introduced on the E-Series ExaScale.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
6.1.1.0	Introduced on the E-Series.														
Related Commands	ip ssh server — enables the secure shell (SSH) server on the system.														

ip telnet source-interface

Set an interface's IP address as the source address in outgoing packets for Telnet sessions.

Z9500

Syntax	<pre>ip telnet source-interface <i>interface</i></pre>
---------------	--

To return to the default setting, use the `no ip telnet source-interface [interface]` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Defaults

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Related Commands

[telnet](#) — telnets to another device.

ip tftp source-interface

Assign an interface's IP address in outgoing packets for TFTP traffic.

Z9500

Syntax	<pre>ip tftp source-interface <i>interface</i></pre> To return to the default setting, use the <code>no ip tftp source-interface <i>interface</i></code> command.	
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: • For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. • For a Port Channel, enter the keyword <code>port-channel</code> then a number. For the C-Series and S-Series, the range is 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
Defaults	The IP address on the system that is closest to the Telnet address is used in the outgoing packets.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4820T.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

line

Enable and configure console and virtual terminal lines to the system. This command accesses LINE mode, where you can set the access conditions for the designated line.

Z9500

Syntax	<code>line {console 0 vty number [end-number]}</code>
Parameters	console 0 Enter the keyword <code>console 0</code> to configure the console port. The console option for the S-Series is <code><0-0></code>. vtty number Enter the keyword <code>vtty</code> then a number from 0 to 9 to configure a virtual terminal line for Telnet sessions. The system supports 10 Telnet sessions. end-number (OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.
Defaults	Not configured
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>E-Series</td><td>Original command</td></tr> </table>	Version	Description	E-Series	Original command
Version	Description				
E-Series	Original command				
Usage Information	You cannot delete a terminal connection.				
Related Commands	access-class — restricts the incoming connections to a particular IP address in an IP access control list (ACL). password — specifies a password for users on terminal lines.				

logging coredump server

Configure the switch to move (upload) a core dump for an application or kernel crash to an external FTP server.

Z9500

Syntax	<code>logging coredump server {<i>ipv4-address</i> <i>ipv6-address</i>} username <i>name</i> password [<i>type</i>] <i>password</i></code>								
Parameters	<table> <tr> <td><i>{ipv4-address ipv6-address}</i></td><td>Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).</td></tr> <tr> <td><i>name</i></td><td>Enter a username to access the target server.</td></tr> <tr> <td><i>type</i></td><td>Enter the password type: - Enter 0 to enter an unencrypted password. - Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm. </td></tr> <tr> <td><i>password</i></td><td>Enter a password to access the target server.</td></tr> </table>	<i>{ipv4-address ipv6-address}</i>	Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).	<i>name</i>	Enter a username to access the target server.	<i>type</i>	Enter the password type: - Enter 0 to enter an unencrypted password. - Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.	<i>password</i>	Enter a password to access the target server.
<i>{ipv4-address ipv6-address}</i>	Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).								
<i>name</i>	Enter a username to access the target server.								
<i>type</i>	Enter the password type: - Enter 0 to enter an unencrypted password. - Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.								
<i>password</i>	Enter a password to access the target server.								
Defaults	Core dumps for kernal and application crashes are stored in the local flash of the Z9500 Control Processor CPU.								
Command Modes	CONFIGURATION								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.				
Version	Description								
9.2(1.0)	Introduced on the Z9500.								

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.0(1.0)</td><td>Introduced on the S5000.</td></tr> </table>	Version	Description	9.0(1.0)	Introduced on the S5000.
Version	Description				
9.0(1.0)	Introduced on the S5000.				
Usage Information	The Z9500 supports full core dumps for kernel crashes. The kernel core dump applies to all Z9500 CPUs and is not enabled by default. To enable full kernel core dumps, enter the <code>logging coredump</code> command in global configuration mode. The kernel core dump is copied to the Control Processor (CP) core-dump directory: <code>flash://CORE_DUMP_DIR/f10_cpu_timestamp.kcore.gz</code> Where <i>cpu</i> specifies a Z9500 CPU and is one of the following values: cp (Control Processor), rp (Route Processor), lp0 (line-card processor 0), lp1 (line-card processor 1), or lp2 (line-card processor 2); <i>timestamp</i> is a text string in the format: <i>yyyymmhhmmss</i> (YearDayMonthHourMinuteSecond). Because flash space may be limited, using the <code>logging coredump server</code> command ensures your crash (application and kernel) files are uploaded successfully and completely to a server. Only a single core-dump server can be configured. Configuration of a new core dump server over-writes any previously configured server.  NOTE: You must disable logging coredump (no <code>logging coredump</code> command) before you configure a new server destination for core dumps. When you enter the <code>logging coredump server</code> command, you are required to enter a password. Use the password of the FTP server where the core files are to be copied. The password can be up to 15 characters; special characters are allowed. After you enter the password, an FTP URL is created with the credentials in the operating system. The CLI monitors core dumps in the unit. On the Z9500, when you enable core dumps of application and kernel crashes to be uploaded to an FTP server, only core dumps from the Control Processor are uploaded to the server. Core-dump files from the Route Processor and line-card CPUs are moved to flash memory on the Control Processor CPU and can be accessed by performing an FTP to the Control Processor core-dump directory: <code>flash://CORE_DUMP_DIR/f10_cpu_timestamp.kcore.gz</code>				

motd-banner

Enable a message of the day (MOTD) banner to appear when you log in to the system.

Z9500

Syntax	<pre>motd-banner</pre> To disable the MOTD banner, use the <code>no motd-banner</code> command.
--------	--

Defaults	Enabled on all lines.																		
Command Modes	LINE																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>E-Series</td><td>Original command</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.12.0	Introduced on the S4810.																		
8.3.11.1	Introduced on the Z9000.																		
8.1.1.0	Introduced on the E-Series ExaScale																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
E-Series	Original command																		

ping

Test connectivity between the system and another device by sending echo requests and waiting for replies.

Z9500

Syntax

```
ping [host | ip-address | ipv6-address] [count {number | continuous}] [datagram-size] [timeout] [source (ip src-ipv4-address) | interface] [tos] [df-bit (y|n)] [validate-reply(y|n)] [outgoing-interface] [pattern pattern] [sweep-min-size] [sweep-max-size] [sweep-interval] [ointerface (ip src-ipv4-address) | interface]
```

Parameters

host	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.
ip-address	(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
ipv6-address	(OPTIONAL) Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

<i>count</i>	Enter the number of echo packets to be sent. The default is 5. • number: from 1 to 2147483647 • continuous: transmit echo request continuously
<i>datagram size</i>	Enter the ICMP datagram size. The range is from 36 to 15360 bytes. The default is 100.
<i>timeout</i>	Enter the interval to wait for an echo reply before timing out. The range is from 0 to 3600 seconds. The default is 2 seconds.
<i>source</i>	Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only. Enter the IP address in A.B.C.D format. • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number: The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Tunnel interface, enter the keyword <code>tunnel</code> then a number from 1 to 16383. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>tos</i>	(IPv4 only) Enter the type of service required. The range is from 0 to 255. The default is 0.
<i>df-bit</i>	(IPv4 only) Enter <code>Y</code> or <code>N</code> for the "don't fragment" bit in IPv4 header. • <code>N</code>: Do not set the "don't fragment" bit. • <code>Y</code>: Do set "don't fragment" bit Default is No.
<i>validate-reply</i>	(IPv4 only) Enter <code>Y</code> or <code>N</code> for reply validation. • <code>N</code>: Do not validate reply data. • <code>Y</code>: Do validate reply data. Default is No.
<i>outgoing-interface</i>	(IPv6 link-local address) Enter the outgoing interface for ping packets to a destination link-local address.
<i>pattern pattern</i>	(IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF. Default: 0xABCD.
<i>sweep-min-size</i>	Enter the minimum size of datagram in sweep range. The range is from 52 to 15359 bytes.

<i>sweep-max-size</i>	Enter the maximum size of datagram in sweep range. The range is from 53 to 15359 bytes.
<i>sweep-interval</i>	Enter the incremental value for sweep size. The range is from 1 to 15308 seconds.
<i>ointerface</i>	(IPv4 only) Enter the outgoing interface for multicast packets. Enter the IP address in A.B.C.D format. - For a Port Channel, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
	Added support for the <code>outgoing-interface</code> option for link-local IPv6 addressing on the S4820T.
8.3.12.0	Added support for the <code>outgoing-interface</code> option for link-local IPv6 addressing on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on the ExaScale.
8.4.1.0	IPv6 pinging available on management interface.
8.3.1.0	Introduced extended ping options.
8.2.1.0	Introduced on the E-Series ExaScale (IPv6).
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).
7.9.1.0	Introduced VRF.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for IPv6 address on the E-Series.

Usage Information

When you enter the `ping` command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for extended commands. For information on ICMP message types, refer to the Usage Information in [deny icmp](#).

The following table provides descriptions for the `ping` command status response symbols displayed in the output.

Symbol	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

Example (IPv4)

```
Dell#ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2
seconds:
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
Dell#
```

Example (IPv6)

```
Dell#ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max =
0/0/0 (ms)
Dell#
```

reload

Reboot the system.

Z9500

Syntax	reload [conditional <i>nvr</i> am- <i>cfg</i> -change]	
Parameters	conditional <i>nvr</i>am-<i>cfg</i>-<i>change</i>	Reload if the condition is true. A configuration change to the nvr
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	9.1(0.0)	Added 'conditional' parameter.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	E-Series	Original command.
Usage Information	If there is a change in the configuration, the system prompts you to save the new configuration. Or you can save your running configuration with the <code>copy running-config</code> command. Use the conditional parameter if any configuration changes made to the nvr	

send

Send messages to one or all terminal line users.

Z9500

Syntax	send [*] [line] [console] [vty]
--------	--

Parameters	*	Enter the asterisk character <code>*</code> to send a message to all tty lines.																		
	line	Send a message to a specific line. The range is from 0 to 11.																		
	console	Enter the keyword <code>console</code> to send a message to the primary terminal line.																		
	vty	Enter the keyword <code>vty</code> to send a message to the virtual terminal.																		
Defaults	none																			
Command Modes	EXEC																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.5.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.12.0	Introduced on the S4810.																			
8.3.11.1	Introduced on the Z9000.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.5.1.0	Introduced on the E-Series.																			
Usage Information	Messages can contain an unlimited number of lines; however, each line is limited to 255 characters. To move to the next line, use <code><CR></code>. To send the message use <code>CTR-Z</code>; to abort a message, use <code>CTR-C</code>.																			

service timestamps

To debug and log messages, add time stamps. This command adds either the uptime or the current time and date.

Z9500

Syntax	<pre>service timestamps [debug log] [datetime [localtime] [msec] [show-timezone] uptime]</pre>
---------------	--

To disable timestamping, use the `no service timestamps [debug | log]` command.

Parameters

debug	(OPTIONAL) Enter the keyword <code>debug</code> to add timestamps to debug messages.
log	(OPTIONAL) Enter the keyword <code>log</code> to add timestamps to log messages with severity from 0 to 6.
datetime	(OPTIONAL) Enter the keyword <code>datetime</code> to have the current time and date added to the message.
localtime	(OPTIONAL) Enter the keyword <code>localtime</code> to include the localtime in the timestamp.
msec	(OPTIONAL) Enter the keyword <code>msec</code> to include milliseconds in the timestamp.
show-timezone	(OPTIONAL) Enter the keyword <code>show-timezone</code> to include the time zone information in the timestamp.
uptime	(OPTIONAL) Enter the keyword <code>uptime</code> to have the timestamp based on time elapsed since system reboot.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

If you do not specify parameters and enter service timestamps, it appears as service timestamps debug uptime in the running-configuration.

To view the current options set for the `service timestamps` command, use the `show running-config` command.

show alarms

View alarms for the system Core, switching core, port modules, fan trays, and power supplies.

Z9500

Syntax	<code>show alarms [threshold]</code>	
Parameters	threshold	(OPTIONAL) Enter the keyword <code>threshold</code> to display the temperature thresholds set for the line cards, RPM, and SFMs.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Examples

```
Dell#show alarms
-- Minor Alarms --
Alarm Type                                         Duration
-----
No minor alarms

-- Major Alarms --
Alarm Type                                         Duration
-----
```



```

PEM 0 in unit 0 down          25 sec
PEM 2 in unit 0 down          6 sec

```

```
Dell#show alarms threshold
```

```
-- System Core --
```

```
-- Temperature Limits (deg C) --
```

	Minor	Minor Off	Major	Major Off	Shutdown
S0	50	45	50	45	N/A
S1	N/A	N/A	N/A	N/A	N/A
S2	50	45	50	45	N/A
S3	50	45	50	45	N/A
S4	40	35	40	35	N/A
S5	50	45	50	45	N/A
S6	67	62	67	62	N/A
S7	68	63	68	63	N/A
S8	66	61	66	61	N/A
S9	66	61	66	61	N/A

```
-- Switching Core --
```

```
-- Temperature Limits (deg C) --
```

	Minor	Minor Off	Major	Major Off	Shutdown
S0	93	86	100	95	105
S1	93	86	100	95	105
S2	93	86	100	95	105
S3	93	86	100	95	105
S4	93	86	100	95	105
S5	93	86	100	95	105

```
-- Port Modules --
```

```
-- Temperature Limits (deg C) --
```

	Minor	Minor Off	Major	Major Off	Shutdown
S0	93	86	100	95	105
S1	93	86	100	95	105
S2	93	86	100	95	105
S3	93	86	100	95	105
S4	93	86	100	95	105
S5	93	86	100	95	105
S6	93	86	100	95	105
S7	93	86	100	95	105
S8	93	86	100	95	105
S9	93	86	100	95	105
S10	93	86	100	95	105

show asf

View statistics about the Alternate Store and Forward (ASF) packets that are transmitted on Z9500 line cards.

Z9500

Syntax	show asf linecard <i>slot-id</i>	
Parameters	linecard <i>slot-id</i>	Enter the slot ID of a Z9500 line card. The range of slot IDs is from 0 to 2.
Defaults	all	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example	<pre>Dell#show asf linecard 0 Processor : CP ----- Received 100% traffic on TenGigabitEthernet 2/2 Total packets: 100 LLC:0, SNAP:0, IP:100, ARP:0, other:0 Unicast:100, Multicast:0, Broadcast:0 Processor : RP1 ----- Received 62% traffic on TenGigabitEthernet 2/2 Total packets: 500 LLC:0, SNAP:0, IP:500, ARP:0, other:0 Unicast:500, Multicast:0, Broadcast:0 Received 37% traffic on TenGigabitEthernet 2/1 Total packets: 300 LLC:0, SNAP:0, IP:300, ARP:0, other:0 Unicast:300, Multicast:0, Broadcast:0 Processor : RP2 ----- No CPU traffic statistics. Dell#</pre>
---------	--

show command-history

Display a buffered log of all commands all users enter along with a time stamp.

Z9500

Syntax `show command-history`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information One trace log message is generated for each command. No password information is saved to this file. A command-history trace log is saved to a file after an RPM failover. Dell Networking TAC analyzes this file to help identify the root cause of an RPM failover.

Example

```
Dell#show command-history
[11/20 15:47:22]: CMD-(CLI):[service password-encryption]by
default from console
[11/20 15:47:22]: CMD-(CLI):[service password-encryption
hostname Force10]by
default from console
- Repeated 3 times.
[11/20 15:47:23]: CMD-(CLI):[service timestamps log
datetime]by default from
console
[11/20 15:47:23]: CMD-(CLI):[hostname Force10]by default from
console
```

```

[11/20 15:47:23]: CMD-(CLI):[enable password 7 *****]by
default from console
[11/20 15:47:23]: CMD-(CLI):[username admin password 7
*****]by default from
console
[11/20 15:47:23]: CMD-(CLI):[enable restricted 7 *****]by
default from console
[11/20 15:47:23]: CMD-(CLI):[protocol spanning-tree rstp]by
default from console
[11/20 15:47:23]: CMD-(CLI):[protocol spanning-tree pvst]by
default from console
[11/20 15:47:23]: CMD-(CLI):[no disable]by default from console
[11/20 15:47:23]: CMD-(CLI):[interface tengigabitethernet
0/1]by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 1.1.1.1 /24]by default
from console
[11/20 15:47:23]: CMD-(CLI):[ip access-group abc in]by default
from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown]by default from
console
[11/20 15:47:23]: CMD-(CLI):[interface tengigabitethernet
0/2]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from
console
[11/20 15:47:23]: CMD-(CLI):[shutdown]by default from console
[11/20 15:47:23]: CMD-(CLI):[interface tengigabitethernet
0/3]by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 5.5.5.1 /24]by default
from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown]by default from
console
[11/20 15:47:23]: CMD-(CLI):[interface tengigabitethernet
0/4]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from
console
[11/20 15:47:23]: CMD-(CLI):[shutdown]by default from console
[11/20 15:47:23]: CMD-(CLI):[interface tengigabitethernet
0/5]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from
console
[11/20 15:47:23]: CMD-(CLI):[shutdown]by default from console
[11/20 21:17:35]: CMD-(CLI):[line console 0]by default from
console
[11/20 21:17:36]: CMD-(CLI):[exec-timeout 0]by default from
console
[11/20 21:17:36]: CMD-(CLI):[exit]by default from console
[11/20 21:19:25]: CMD-(CLI):[show command-history]by default
from console
Dell#

```

show command-tree

Display the entire CLI command tree, and optionally, display the utilization count for each command and its options.

Z9500

Syntax	show command-tree [count no]	
Parameters	count	Display the command tree with a usage counter for each command.
	no	Display all of the commands that may be preceded by the keyword no, which is the keyword used to remove a command from the running-configuration.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced.

Usage Information	Reload the system to reset the command-tree counters.
-------------------	---

Example	<pre>Dell#show command-tree count ! Enable privilege mode: enable command usage:3 <0-15> option usage: 0 exit command usage:1 show command-tree command usage:9 count option usage: 3 show version command usage:1 ! Global configuration mode:</pre>
---------	---

```

aaa authentication enable command usage:1
WORD      option usage: 1
default   option usage: 0
enable    option usage: 0
line      option usage: 0
none      option usage: 0
radius    option usage: 1
tacacs+   option usage: 0

```

show console lp

View the buffered boot-up log of a line card, Route Processor or Control Processor CPU, including background resets, calls, and initialization, on the console.

Z9500

Syntax	<code>show console {lp <i>slot-id</i> rp cp}</code>	
Parameters	lp<i>slot-id</i>	Enter a line-card slot number to view the boot-up log of a line-card (LP) processor. The range of Z9500 slot IDs is from 0 to 2.
	rp	Enter the <code>rp</code> keyword to view the boot-up log for the Route Processor CPU.
	cp	Enter the <code>cp</code> keyword to view the boot-up log for the Control Processor CPU.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.



CAUTION: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show cpu-traffic-stats

View CPU traffic statistics.

Z9500

Syntax	<code>show cpu-traffic-stats [cp rp linecard {slot-id}]</code>	
Parameters	cp	Enter the keyword <code>cp</code> to display traffic statistics on the Control Processor CPU.
	rp	Enter the keyword <code>rp</code> to display traffic statistics on the Route Processor CPU.
	linecard slot-id	Enter the slot ID of the line card for which you want to display traffic statistics. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to display traffic statistics for all line cards.
Defaults	Display CPU traffic statistics for all Z9500 CPUs (Control Processor, Route Processor, and line cards).	
Command Modes	EXEC	
Example	<code>Dell#show cpu-interface-stats</code>	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	6.2.1.1	Introduced on the E-Series.
Version	Description				
6.2.1.1	Introduced on the E-Series.				
Usage Information	Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the <code>debug cpu-traffic-stats</code> command is executed; not from the system bootup.  NOTE: After debugging is complete, use the <code>no debug cpu-traffic-stats</code> command to shut off traffic statistics collection.				
Example	<pre>Dell#show cpu-traffic-stats Processor : CP ----- Received 100% traffic on fortyGigE 2/12 Total packets:8 LLC:0, SNAP:0, IP:5, ARP:0, other:3 Unicast:5, Multicast:3, Broadcast:0 Processor : RP ----- Received 100% traffic on fortyGigE 2/12 Total packets:168 LLC:0, SNAP:0, IP:165, ARP:0, other:3 Unicast:42, Multicast:126, Broadcast:0</pre>				
Related Commands	debug cpu-traffic-stats — enables CPU traffic statistics for debugging.				

show cpu-interface-stats

View CPU interface statistics.

Z9500

Syntax	show <code>cpu-interface-stats</code> [<code>cp</code> <code>rp</code> <code>linecard {0-2}</code> <code>all</code>]	
Parameters		
	cp	Enter the keyword <code>cp</code> to display the interface statistics only from the Control Processor.
	rp	Enter the keyword <code>rp</code> to display the interface statistics only from the Route Processor.
	linecard <i>slot-id</i>	Enter the <code>linecard slot-id</code> parameters to display the interface statistics only from a specified line card. The range of line-card slot IDs is from 0 to 2.
	all	Enter the keyword <code>all</code> to display the interface statistics from all Z9500 CPUs, including the Control Processor, Route Processor, and line cards.

Defaults	Display interface statistics from all Z9500 CPUs.																
Command Modes	EXEC																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Introduced on the S4810.																
8.3.11.1	Introduced on the Z9000.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces.																
Example	<pre> Dell#show cpu-traffic-stats cp -- Partybus ethernet statistics -- Link state : Up Recv Interrupts/Polls: 0 Recv Packets : 2027080 Transmit Packets : 590000 Recv Desc Error : 0 Transmit Desc Error : 0 Recv Out of Mem : 0 Transmit Out of Mem : 0 Recv Upper Layer Full: 0 Transmit Pause Pkts : 0 Recv Other Error : 0 Transmit Other Error: 0 Recv Restarts : 0 Recv Restarts Fatal : 0 -- Dataplane ethernet statistics -- bc pci driver statistics for device: rxHandle :0 noMhdr :0 noMbuf :0 noClus :0 recvd :0 dropped :0 recvToNet :0 rxError :0 rxDatapathErr :0 rxPkt (COS0) :0 rxPkt (COS1) :0 </pre>																

```

rxPkt(COS2)      :0
rxPkt(COS3)      :0
rxPkt(COS4)      :0
rxPkt(COS5)      :0
rxPkt(COS6)      :0
rxPkt(COS7)      :0
rxPkt(UNIT0)     :0
rxPkt(UNIT1)     :0
rxPkt(UNIT2)     :0
rxPkt(UNIT3)     :0
transmitted      :0
txRequested      :0
noTxDesc         :0
txError          :0
txReqTooLarge    :0

txDatapathErr    :0
txPkt(COS0)      :0
txPkt(COS1)      :0
txPkt(COS2)      :0
txPkt(COS3)      :0
txPkt(COS4)      :0
txPkt(COS5)      :0
txPkt(COS6)      :0
txPkt(COS7)      :0
txPkt(UNIT0)     :0
txPkt(UNIT1)     :0
txPkt(UNIT2)     :0
txPkt(UNIT3)     :0
-- OOB ethernet statistics --
Link state       : N/A
Recv Interrupts/Polls: 0
Recv Packets     : 2269516   Transmit Packets :
549631
Recv Desc Error  : 0         Transmit Desc
Error : 0
Recv Out of Mem  : 0         Transmit Out of
Mem : 0
Recv Upper Layer Full: 0     Transmit Pause
Pkts : 0
Recv Other Error : 0         Transmit Other
Error: 0
Recv Restarts    : 0
Recv Restarts Fatal : 0
-- Thread info ...i .. command output --
pthread      state      PRI que state  cntxt sw name
UTIME STIME
0xb8fbe000   *running    154 -----f      779 CLI
0.09 0.09
0xb904e000   running      54 -c----P--f    13163 sSThread
1.01 1.60
0xb9030000   running      54 -----P--f      6 tSnmpd
0.00 0.00
0xb902e000   cond_wait     54 -c-C-W---f     1 tSnmpTmr
0.00 0.00
0xb90ac000   running      54 -----P--f     88 auxd
0.00 0.00
0xb9125000   select_wait   154 ----RW---f    2455 CLIIInit
0.31 0.43
0xb92f0000   select_wait   54 ----RW---f     86 DHCLIENT
0.01 0.00
0xb931a000   select_wait   54 ----RW---f      1 cms
0.00 0.00
0xb93a3000   select_wait   54 ----RW---f    6672 portmirr

```

```

0.24 0.25
0xb93bd000 select_wait 54 ----RW---f      2 cfgDataS
0.00 0.00
0xb93d1000 select_wait 54 ----RW---f      2 sysCompM
0.00 0.00
0xb9470000 select_wait 54 ----RW---f    166043 statMgr
7.09 6.28
0xb94c8000 running      54 -----P--f  1579998 sflCp
37.86 43.13
0xb9560000 running      54 -----P--f    21857 snmp
0.95 1.69
0xb99e0000 running      54 -----P--f     25 usm
0.00 0.02
0xb957f000 running      54 -----P--f    72691 dpi_daem
4.50 4.16
0xb9594000 select_wait 54 ----RW---f      2 dpi
0.00 0.00
0xb95a8000 select_wait 54 ----RW---f   376512 diagmgr
3.80 6.18

```

```

-- netstat -i command output --
Name Mtu Network Address Ipkts Ierrs
Opkts Oerrs Colls Drops
bc0 1500 0 0 00:00:00:00:00:00 0 0
0 0 0 0
mul0 1500 0 0 00:00:00:00:00:00 0 0
0 0 0 0
wm0 1500 0 0 74:86:7a:ff:6f:24 2240632 17
608097 0 0 0
wm1 9710 0 0 74:86:7a:ff:6e:a0 0 0
0 0 0 0
lo0 33192 0 0 212314 0
212314 0 0 0
lo0 33192 ::1/128 ::1 212314 0
212314 0 0 0
lo0 33192 127.0.0/24 127.0.0.1 212314 0
212314 0 0 0
backp 1500 0 0 74:86:7a:ff:6f:24 2027232 0
590069 0 0 0
backp 1500 127.10.10/24 RPM0-CP 2027232 0
590069 0 0 0
backp 1500 127.10.10.43/ LC-3 2027232 0
590069 0 0 0
rcpu0 9000 0 0 74:86:7a:ff:6e:a0 0 0
0 0 0 0
cop0 1500 0 0 00:00:00:00:00:00 0 0
0 0 0 0
ifdbg 2000 0 0 0 0
0 0 0 0
ifarp 2000 0 0 0 0
0 0 0 0
ificm 2000 0 0 0 0
0 0 0 0
ifdbg 2000 0 0 0 0
0 0 0 0
ifacl 2000 0 0 0 0
0 0 0 0
if6db 2000 0 0 0 0
0 0 0 0
if6db 2000 0 0 0 0

```

show debugging

View a list of all enabled debugging processes.

Z9500

Syntax `show debugging`

Command Modes EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.3.11.1	Introduced on the Z9000.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series
	E-Series	Original command.

Example

```
Dell#show debugging
Generic IP:
  IP packet debugging is on for
    ManagementEthernet 0/0
    Port-channel 1-2
    Port-channel 5
    TenGigabitEthernet 0/0-3,5-6,10-11,20
    TenGigabitEthernet 1/0-1,5-6,10-11,15,17,19,21
  ICMP packet debugging is on for
    TenGigabitEthernet 1/0,2,4,6,8,10,12,14,16
  DHCP Server:
    DHCP server packet debugging on
Dell#
```

show environment

View system component status (for example, temperature or power).

Z9500

Syntax	show environment [fan pem thermal-sensors all]																
Parameters	fan	Enter the keyword all to display status information only on the fan units.															
	pem	Enter the keyword all to display status information only on the power supplies and power usage.															
	thermal-sensors	Enter the keyword all to display only temperatures and thresholds for the system and switching core, and port modules.															
	all	Enter the keyword all to display status information on all components.															
Default	Display status information on all system components.																
Command Modes	- EXEC - EXEC Privldge																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>7.8.1.0</td><td>The output of the show environment fan command for the S-Series is changed to display fan speeds instead of showing the fan status as up or down.</td></tr><tr><td>7.6.1.0</td><td>Introduced for the S-Series. S-Series options and output differ from the C-Series/E-Series version.</td></tr></table>			Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.8.1.0	The output of the show environment fan command for the S-Series is changed to display fan speeds instead of showing the fan status as up or down.	7.6.1.0	Introduced for the S-Series. S-Series options and output differ from the C-Series/E-Series version.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Introduced on the S4810.																
8.3.11.1	Introduced on the Z9000.																
7.8.1.0	The output of the show environment fan command for the S-Series is changed to display fan speeds instead of showing the fan status as up or down.																
7.6.1.0	Introduced for the S-Series. S-Series options and output differ from the C-Series/E-Series version.																
Usage Information	The following examples show sample output of the show environment command.																
Examples	<pre>Dell#show environment pem -- Power Supplies -- Unit Bay Status Type FanStatus FanSpeed(rpm) Power Usage</pre>																

```

(W)
-----
0    0    down    AC    up        1376        0.0
0    1    up      AC    up        18848       666.0
0    2    down    AC    up        1312        0.0
0    3    up      AC    up        18880       643.0

Dell#show environment fan

-- Fan Status --
Unit   Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-----
0      0     up          up      5263    up      5292
0      1     up          up      5274    up      5317
0      2     up          up      5256    up      5292
0      3     up          up      5278    up      5328
0      4     up          up      5270    up      5320

Speed in RPM

Dell#show environment thermal-sensors

-- Thermal Sensor Readings (deg C) --
Module  S0    S1    S2    S3    S4    S5
S6      S7    S8    S9    S10
-----
System Core      33    33    34    33    28    39
25      36    39    39    -
Switching Core  100[M] 46    47    45    44    45
-        -    -    -    -
Port Modules    49    101[M] 60    49    62    52
78      55    53    50    46

Threshold crossed [m]: minor [M]: major, [S]: shutdown

```

show inventory

Display the switch type, components (including media), and Dell Networking OS version, including hardware identification numbers and configured protocols.

Z9500

Syntax	show inventory [media slot-id]	
Parameters	media slot-id	(OPTIONAL) Enter the keyword <code>media</code> to display pluggable media inventory for a specified line-card slot. Valid slot ID are from 0 to 2.
Defaults	none	
Command Modes	CONFIGURATION	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.4	Output expanded to include Piece Part ID (PPID) and eSR4 optics.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced this version of the command for S-Series. S-Series output differs from E-Series.

Usage Information

Use the `show inventory` command to display information about installed pluggable media (QSFP, SFP) on a Z9500 line card. If no optics are installed in the fiber ports, the output displays *Media not present or accessible*.

Example (Z9000)

```
ct-z9000-2#show inventory
System Type       : Z9000
System Mode       : 1.0
Software Version  : 8.3.11.3b

Unit Type          Serial Number Part Number  Rev Piece
Part ID
Ver Service Tag
-----
----

*   0 Z9000-01-40GE-AC Z8FX113100314 7520052401 E
MY-08R4VK-75412-1BA-0474 A00 ABC1234
    0 Z9000-PWR-AC      N/A          N/A      N/A N/A
    0 Z9000-FAN         Z5FX112500170 7520051702 A
MY-08R4VK-75412-1BA-0474 A00 ABC1234
    0 Z9000-FAN         Z5FX113300293 7520051702 A   N/A
    0 Z9000-FAN         Z5FX113300160 7520051702 A
MY-08R4VK-75412-1BA-0474 A00 ABC1234
    0 Z9000-FAN         Z5FX113300136 7520051702 A
MY-08R4VK-75412-1BA-0474 A00 ABC1234

* - Management Unit

Dell#show inventory media
Slot  Port  Type      Media
Serial Number      F10Qualified
-----
-----
      2    0   QSFP      40GBASE-CR4-1M
APF12380010GM4     Yes
      2    4             Media not present or accessible
      2    8             Media not present or accessible
      2   12             Media not present or accessible
      2   16   QSFP      40GBASE-SR4
7503825D0169      Yes
```

2	20		Media not present or accessible
2	24	QSFP	40GBASE-CR4-1M
APF12380010GM4			Yes
2	28		Media not present or accessible
2	32		Media not present or accessible
2	36		Media not present or accessible
2	40	QSFP	40GBASE-SR4
7503825H006J		Yes	
2	44		Media not present or accessible

Related Commands

- [show interfaces](#) — displays the interface configuration.
- [show interfaces transceiver](#) — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show memory

View current memory usage on the system.

Z9500

Syntax

```
show memory [cp | rp | linecard {slot-id | all}]
```

Parameters

- | | |
|-------------------------|---|
| cp | Enter the keyword <code>cp</code> to display memory usage on the Control Processor CPU. |
| rp | Enter the keyword <code>rp</code> to display memory usage on the Route Processor CPU. |
| linecard slot-id | Enter the slot ID of the line card for which you want to display memory usage. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to display memory usage on all line cards. |

Command Modes

- EXEC
- EXEC Privilege

Defaults

Display memory usage on all Z9500 CPUs (Control Processor, Route Processor, and line cards).

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

The output for `show memory` displays the memory usage of the line-card processor (LP) part (sysdlp) of the system. The sysdlp is an aggregate task that handles all the tasks running on the LP.

The total counter size in `show memory` and `show processes memory` differs based on which OS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.
- In the `show processes memory` output, the memory size is equal to the size of the application processes plus the size of the system processes.

Examples

```
Dell#show memory
```

```

      Statistics On  CP Processor
      =====
      Total (b)      Used (b)      Free (b)      Lowest (b)
Largest (b)
3203928064          6953130      3196974934      3196941986
3196974934
      Statistics On  RP Processor
      =====
      Total (b)      Used (b)      Free (b)      Lowest (b)
Largest (b)
3203928064          17806442      3186121622      3186088674
3186121622

```

```

Dell#show memory cp
      Total (b)      Used (b)      Free (b)      Lowest (b)
Largest (b)
3203928064          6953130      3196974934      3196974934
3196974934

```

```

Dell#show memory rp
      Total (b)      Used (b)      Free (b)      Lowest (b)
Largest (b)
3203928064          17174702      3186753362      3186753362
3186753362

```

```

Dell#show memory lp 2
      Total (b)      Used (b)      Free (b)      Lowest (b)
Largest (b)
3203928064          8555410      3195372654      3195372654
3195372654FTOS#

```

“Lowest” displays the memory usage the system went to in the lifetime of the system. Indirectly, it indicates the maximum usage in the lifetime of the system: Total minus Lowest.

“Largest” displays the current largest available. This relates to the block size and is not related to the amount of memory on the system.

show processes cpu

View information on CPU usage for processes running in the system.

Z9500

Syntax	<pre>show processes cpu [cp rp linecard {slot-id [0-2] all}] [summary details]</pre>	
Parameters	cp	Enter the keyword <code>cp</code> to view CPU usage for the Control Processor.
	rp	Enter the keyword <code>rp</code> to view CPU usage for the Route Processor.
	linecard slot-id [0-2]	Enter the slot ID of the line card for which you want to view CPU usage. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to display CPU usage for all line cards. The optional line card 0-2 parameter displays tasks in order of the highest CPU usage in the past five seconds.
	all	Enter the keyword <code>all</code> to display usage information for all Z9500 CPUs: Control Processor, Route Processor, and line cards.
	summary	Enter the keyword <code>summary</code> to view a summary of CPU usage.
	details	Enter the keyword <code>details</code> to view detailed information about CPU usage.
Command Modes	- EXEC - EXEC Privilege	
Defaults	Display detailed information on CPU usage for all Z9500 CPUs (Control Processor, Route Processor, and line cards).	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.

Version	Description
7.5.1.0	Introduced on the C-Series.

Usage Information In the following example, the CPU utilization for the last five seconds is 10%/0%. The first number (10%) is the CPU utilization for the last five seconds. The second number (0%) indicates the percent of CPU time spent at the interrupt level.

Example: show processes cpu lp

```
Dell#show processes cpu lp 2 30

CPU utilization for five seconds: 10%/0%; one minute: 10%;
five minutes: 10%
PID      Runtime(ms)   Invoked    uSecs    5Sec   1Min   5Min
TTY      Process
0x00000000 995730    99573    10000    10.08% 10.10% 10.12%
0 system
0x0000012e 54470     5447     10000     0.00%  0.43%  0.46%
0 sysdlp
0x00000125 0         0         0         0.00%  0.00%  0.00%
0 flashmntr
0x000000c9 10        1         10000     0.00%  0.00%  0.00%
0 inetd
0x0000007b 30        3         10000     0.00%  0.00%  0.00%
0 sh
0x0000004b 20        2         10000     0.00%  0.00%  0.00%
0 sh
0x0000001f 20        2         10000     0.00%  0.00%  0.00%
0 mount_mfs
0x0000001a 150       15        10000     0.00%  0.00%  0.00%
0 mount_mfs
----- More -----
```

```
Dell#show processes cpu lp 2 details

CPU utilization for five seconds: 10%/0%; one minute: 10%;
five minutes: 10%
PID      Runtime(ms)   Invoked    uSecs    5Sec   1Min   5Min
TTY      Process
0x00000000 976300    97630    10000    10.47% 10.14% 10.14%
0 system
0x0000012e 53570     5357     10000     0.00%  0.46%  0.45%
0 sysdlp
0x0000012e 1260      126      10000     0.00%  0.02%  0.01%
0 diagagt
0x0000012e 0         0         0         0.00%  0.00%  0.00%
0 debugagt
0x0000012e 10        1         10000     0.00%  0.00%  0.00%
0 F10StkMgr
0x0000012e 0         0         0         0.00%  0.00%  0.00%
0 envmgr
0x0000012e 1370      137      10000     0.00%  0.02%  0.01%
0 lcMgr
0x0000012e 140       14       10000     0.00%  0.00%  0.00%
0 dla
0x0000012e 1170      117      10000     0.00%  0.00%  0.01%
0 sysAdmTsk
0x0000012e 40570     4057     10000     0.40%  0.43%  0.41%
0 timerMgr
0x0000012e 570       57       10000     0.00%  0.00%  0.01%
0 PM
0x0000012e 15070     1507     10000     0.20%  0.15%  0.17%
```

```

0          KP
0x0000012e      10          1      10000      0.00%      0.00%      0.00%
0          evagt
0x0000012e      710          71      10000      0.00%      0.00%      0.00%
0          ipc
0x0000012e      90          9      10000      0.00%      0.00%      0.00%
0 sysReaper
0x0000012e      70          7      10000      0.00%      0.00%      0.00%
0          tme
0x0000012e      0          0          0      0.00%      0.00%      0.00%
0 ttraceIpFlow
0x0000012e      0          0          0      0.00%      0.00%      0.00%
0 linkscan_user_t
0x0000012e      310          31      10000      0.00%      0.00%      0.00%
0 tHeartbeat
0x0000012e      0          0          0      0.00%      0.00%      0.00%
0          tDDB
0x0000012e      50          5      10000      0.00%      0.00%      0.00%
0          GC
0x0000012e      0          0          0      0.00%      0.00%      0.00%
0 isrTask
0x0000012e      10          1      10000      0.00%      0.00%      0.00%
0 bshell_reaper_t
0x0000012e      0          0          0      0.00%      0.00%      0.00%
0 tSysLog
0x0000012e      1170          117      10000      0.00%      0.00%      0.01%
0 tTimerTask
0x0000012e      29130          2913      10000      0.40%      0.31%      0.33%
0 tExcTask
0x0000012e      40          4      10000      0.00%      0.00%      0.00%
0 tLogTask
0x0000012e      9060          906      10000      0.20%      0.00%      0.00%
0 tUsrRoot
----- More -----

```

**Example: show
processes cpu
rp**

```

Dell#show processes cpu rp

CPU utilization for five seconds: 0%/0%; one minute: 0%; five
minutes: 0%
PID   Runtime(ms)   Invoked   uSecs   5Sec   1Min   5Min   TTY   Process
496    20             2         10000   0.00%  0.00%  0.00%  0     ofmgr
392    20             2         10000   0.00%  0.00%  0.00%  0     ndpm
160    30             3         10000   0.00%  0.00%  0.00%  0     vrrp
126    20             2         10000   0.00%  0.00%  0.00%  0     frvp
154    50             5         10000   0.00%  0.00%  0.00%  0     xstp
118    10             1         10000   0.00%  0.00%  0.00%  0     pim
434    10             1         10000   0.00%  0.00%  0.00%  0     igmp
429    100            10         10000   0.00%  0.00%  0.00%  0     ipml
170    10             1         10000   0.00%  0.00%  0.00%  0     mrtm
294    100            10         10000   0.00%  0.00%  0.00%  0     l2mgr
98     20             2         10000   0.00%  0.00%  0.00%  0     l2pm
389    40             4         10000   0.00%  0.00%  0.00%  0     arpm
367    10             1         10000   0.00%  0.00%  0.00%  0     lacp
349    10             1         10000   0.00%  0.00%  0.00%  0     tnlmgr
329    10             1         10000   0.00%  0.00%  0.00%  0     otm
333    50             5         10000   0.00%  0.00%  0.00%  0     dsm
323    30             3         10000   0.00%  0.00%  0.00%  0     rtm
315    10             1         10000   0.00%  0.00%  0.00%  0     rip
309    20             2         10000   0.00%  0.00%  0.00%  0     acl
302    460            46         10000   0.00%  0.00%  0.00%  0     sysd
263    0              0          0       0.00%  0.00%  0.00%  0     sysmon
296    0              0          0       0.00%  0.00%  0.00%  0
flashmntr

```

```

198      0      0      0  0.00% 0.00% 0.00%  0  inetd
----- More -----

```

Example: show processes cpu summary

```

Dell#show processes cpu summary

CPU utilization    5Sec    1Min    5Min
-----
CP                43%     42%     40%
RP                0%      0%      0%

```

show processes ipc

Display the IPC messaging used internally between Dell Networking OS processes.

Z9500

Syntax

```

show processes ipc [recv-stats | send-stats] [cp | rp |
linecard {slot-id | all}]

```

Parameters

recv-stats	Enter the keyword <code>recv-stats</code> to display information on IPC receiver-side messages.
send-stats	Enter the keyword <code>send-stats</code> to display information on IPC sender-side messages.
cp	Enter the keyword <code>cp</code> to view IPC message statistics on the Control Processor CPU.
rp	Enter the keyword <code>rp</code> to view IPC message statistics on the Route Processor CPU.
linecard slot-id	Enter the slot ID of the line card for which you want to view IPC message statistics. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to view IPC statistics for all line cards.

Defaults

Display IPC message statistics on all Z9500 CPUs: Control Processor, Route Processor, and line cards.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

Important Points:

- Use `show processes ipc` commands only when you are working directly with Dell Technical Support to troubleshoot a problem.

Example: show processes ipc send-stats

```
Dell#show processes ipc send-stats rp
IPC Send Statistics on RP
Memory Used by Send DB on this processor: 1451880 bytes
SeqNo - Last sent guaranteed IPC pkt sequence no from this
source to destination
Success - No of successfull guaranteed IPC packets sent from
source to destination
1st-R - No of first retry attempts
2nd-R - No of second retry attempts
Fails - No of guaranteed IPC pkts that could not be
transmitted
RTT(ms) - Avg. Round Trip time for guaranteed IPC packets in
millisecs
NonG-S - No of non-guaranteed IPC pkts succesfully sent. This
does not include those sent by SWP
NonG-F - No of non-guaranteed IPC pkt transmission failures
SWP-S - No of non-guaranteed SWP IPC pkts succesfully sent
SWP-F - No of non-guaranteed SWP IPC pkt transmission failures
```

Source->	Destination	SeqNo	Success	1st-R	
2nd-R	Fails	RTT(ms)	NonG-S	NonG-F	SWP-S
SWP-FIPC: 1 ->		TME: 1	1561		3
0	0	0	2	0	0
0	0				
IPC: 1 ->		IPC: 0	37025		0
0	0	0	1107		0
0	0				
EVENTLOGAGENT: 1 ->		TME: 1	18888		0
0	0	0	1		0
0	0				
EVENTLOGAGENT: 1 ->		TME: 1	18888		0
0	0	0	1		0
0	0				
EVENTLOGAGENT: 1 ->		TME: 1	18888		0
0	0	0	1		0
0	0				
EVENTLOGAGENT: 1 ->		TME: 1	18888		0
0	0	0	1		0
0	0				
SYSADMTSK: 1 ->		TME: 1	26574		1
0	0	0	0		0
0	0				

Example: show
processes ipc
recv-stats

	Source->		Destination	SeqNo
HiWtmk(%)	M-SkSize	NonG-Rcvd	Pri-Dr	SkFull-Dr
	TME: 0 ->		TME: 5	0
0	129024	1	0	0
	TME: 5 ->		LCMGR: 2	0
0	129024	1	0	0
	IPC: 0 ->		IPC: 5	0
0	129024	1084	0	0
	IPC: 5 ->		TME: 5	58307
0	129024	0	0	0
	CLI: 0 ->		SYSADMTSK: 5	0
0	129024	11	0	0
	CHMGR: 0 ->		LCMGR: 2	53689
0	129024	4	0	0
	LCMGR: 2 ->		TME: 5	3906
0	129024	1	0	0
	LCMGR: 2 ->		EVENTLOGAGENT: 5	0
0	129024	1	0	0
EVENTLOGAGENT: 5 ->			TME: 5	0
0	129024	1	0	0
	DIAGMGR: 0 ->		DIAGAGT: 5	0
0	129024	1	0	0
	DIAGAGT: 5 ->		TME: 5	7899
0	129024	0	0	0
	DIAGAGT: 5 ->		EVENTLOGAGENT: 5	0
0	129024	1	0	0
	EVHDLR: 0 ->		LCMGR: 2	0
0	129024	1	0	0
	EVHDLR: 0 ->		IFAGT: 2	0
0	129024	1	0	0
	DNLDAGENT: 5 ->		TME: 5	4759

1	129024	0	0	0	
	DNLDAGENT: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	SYSADMTSK: 5 ->		TME: 5		40252
0	129024	0	0	0	
	SYSADMTSK: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	PMMGR: 5 ->		TME: 5		62298
0	129024	0	0	0	
	PMMGR: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	KPLR: 5 ->		TME: 5		36259
0	129024	0	0	0	
	KPLR: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	KPLR: 5 ->		PMMGR: 5		604
0	129024	0	0	0	
	TIMERMGR: 5 ->		TME: 5		14202
0	129024	0	0	0	
	DEBUGAGNT: 5 ->		TME: 5		32
1	129024	0	0	0	
	DEBUGAGNT: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	F10STKMGR: 5 ->		TME: 5		23990
0	129024	0	0	0	
	F10STKMGR: 5 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	ENVMGR: 5 ->		TME: 5		22188
1	129024	0	0	0	
	ACL: 0 ->		ACL_AGENT: 2		24998
0	184320	8	0	0	
	ACL_AGENT: 0 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	ACL_AGENT: 2 ->		TME: 5		18120
0	129024	0	0	0	
	ACL_AGENT: 2 ->		DSAGT: 2		35450
0	129024	0	0	0	
	ACL_AGENT: 2 ->		FRRPAGT: 2		36661
0	163840	0	0	0	
	IFAGT: 2 ->		TME: 5		17874
0	129024	0	0	0	
	IFAGT: 2 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	RTM: 0 ->		FIBAGT: 2		0
1	131072	5	0	0	
	RTM: 0 ->		FIB6: 2		0
0	131072	3	0	0	
	FIBAGT: 2 ->		TME: 5		15595
0	129024	0	0	0	
	FIBAGT: 2 ->		EVENTLOGAGENT: 5		0
0	129024	1	0	0	
	FIBAGT: 2 ->		TNLAGT: 2		3950
0	129024	0	0	0	
	DIFFSERV: 0 ->		ACL_AGENT: 2		11562
2	184320	0	0	0	
	DIFFSERV: 0 ->		DSAGT: 2		0
0	129024	10	0	0	
	ARPMGR: 0 ->		FIBAGT: 2		0
0	129024	1	0	0	
	MACMGR: 0 ->		MACAGENT: 2		0
0	129024	7	0	0	
	DSAGT: 2 ->		TME: 5		35450
0	129024	0	0	0	
	DSAGT: 2 ->		EVENTLOGAGENT: 5		0

0 129024 1 0 0
----- More -----

show processes ipc flow-control

Display Single Window Protocol Queue (SWPQ) statistics.

Z9500

Syntax	<code>show processes ipc flow-control [cp rp linecard {slot-id all}]</code>	
Parameters	cp	Enter the keyword <code>cp</code> to view SWPQ statistics for the Control Processor CPU.
	rp	Enter the keyword <code>rp</code> to view SWPQ statistics for the Route Processor CPU.
	linecard slot-id	Enter the slot ID of the line card for which you want to view SWPQ statistics. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to view SWPQ statistics for all line cards.
Defaults	Display SWPQ statistics on all Z9500 CPUs (Control Processor, Route Processor, and line cards).	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

Field	Description
Source QID /Tx Process	Source Service Identifier
Destination QID/Rx Process	Destination Service Identifier
Cur Len	Current number of messages enqueued
High Mark	Highest number of packets in the queue at any time
Timeout	Timeout count
Retries	Number of retransmissions
Msg Sent	Number of messages sent
Ack Rcvd	Number of messages acknowledged
Available Retra	Number of retries left
Max Retra	Number of retries allowed

Important Points:

- The SWP provides flow control-based reliable communication between the sending and receiving software tasks.
- A sending task enqueues messages into the SWP queue³ for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the SWP-2-NOMORETIMEOUT timeout message is generated.
- A retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example

```
Dell#show processes ipc flow-control cp
```

Q Statistics on CP Processor						
TxProcess		RxProcess		Cur	High	Time
Retr	Msg	Ack	Aval	Max Len	Mark	Out
ies	Sent	Rcvd	Retra	Retra		
	DHCP0	ACL0		0	1	1
1	1	1	25	25		
	DHCP0	IPMGR0		0	0	0
0	0	0	25	25		
	DHCP0	IPMGR1		0	0	0
0	0	0	25	25		
	DHCP0	IFMGR0		0	0	0
0	0	0	25	25		
	IPMGR0	NDPM0		0	0	0
0	0	0	60	60		
	IFMGR0	FEFD0		0	10	0
0	12	12	60	60		
	IFMGR0	SNMP0		0	1	0
0	1	1	60	60		
	IFMGR0	SFL_CP0		0	20	0
0	26	26	60	60		

	IFMGR0	PORTMIRRO		0	8	0
0	9	9 60	60			
	IFMGR0	EVENTTERMLOG0		0	1	0
0	1	1 60	60			
	IFMGR0	IPSECMGR0		0	8	0
0	11	11 60	60			
	IFMGR0	DHCP0		0	8	0
0	11	11 60	60			
	IFMGR0	IPMGR0		0	29	0
0	36	36 60	60			
	IFMGR0	IFAGT3		0	1	0
0	2	2 60	60			
	IFAGT3	IFMGR0		0	1	0
0	1	1 60	60			
	IFMGR0	OFMGR0		0	16	1
1	21	21 60	60			
	IFMGR0	ACL0		0	8	0
0	14	14 60	60			
	IFMGR0	VRRP0		0	10	0
0	17	17 60	60			
	IFMGR0	PIM0		0	1	0
0	1	1 5	5			
	IFMGR0	MACMGR0		0	0	0
0	0	0 60	60			
	IFMGR0	L2PM0		0	29	0
0	40	40 60	60			
	IFMGR0	DIFFSERV0		0	51	0
0	67	67 60	60			
	IFMGR0	RTM0		0	9	0
0	11	11 60	60			
	IFMGR0	LLDP0		0	12	0
0	12	12 60	60			
	IFMGR0	MRTM0		0	10	0
0	10	10 60	60			
	IFMGR0	IPMGR1		0	33	0
0	33	33 60	60			
	IFMGR0	LACP0		0	23	0
0	23	23 60	60			
	PORTMIRRO	ACL_AGENT2		0	0	0
0	0	0 50	50			
	IFMGR0	IGMP0		0	0	0
0	0	0 50	50			
	IFMGR0	IFAGT2		0	1	0
0	1	1 60	60			

show processes memory

View information about memory usage for processes running in the system.

Z9500

Syntax

```
show processes memory [cp | rp | linecard {slot-id | all |
summary}]
```

Parameters

cp

Enter the keyword **cp** to view memory usage for the Control Processor.

	rp	Enter the keyword <code>rp</code> to view memory usage for the Route Processor.
	linecard <i>slot-id</i>	Enter the slot ID of the line card for which you want to view CPU memory usage. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to display memory usage on all line card CPUs. Enter <code>linecard summary</code> to display a summary of memory usage on all line card CPUs.
Command Modes	- EXEC - EXEC Privilege	
Defaults	Display detailed information on memory usage on all Z9500 CPUs (Control Processor, Route Processor, and line cards).	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.3.11.1	Introduced on the Z9000.
	8.1.1.2	Introduced on the E-Series ExaScale E600i.
	8.1.1.0	Introduced on the E-Series ExaScale E1200i.
	7.5.1.0	Introduced on the C-Series.
Usage Information	show processes memory output	Description
	Field	
	Total:	Total system memory available
	MaxUsed:	Total maximum memory used ever (history indicated with a time stamp)
	CurrentUsed:	Total memory currently in use
	CurrentFree:	Total system memory available
	SharedUsed:	Total used shared memory
	SharedFree:	Total free shared memory
	PID	Process ID
	Process	Process Name
	ResSize	Actual resident size of the process in memory
	Size	Process test, stack, and data size
	Allocs	Total dynamic memory allocated

show processes Description

memory output

Field

Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

The output for `show process memory` displays the memory usage statistics running on the CP part (sysd) of the system. The sysd is an aggregate task that handles all the tasks running on the Control Processor.

The total counter size in `show memory` and `show processes memory` differs based on which OS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.
- In the `show processes memory` output, the memory size is equal to the size of the application processes plus the size of the system processes.

Example: show processes memory cp

```
Dell#show processes memory
Total      : 3203928064, MaxUsed      : 804720640 [01/27/2014
06:16:44]
CurrentUsed: 804720640, CurrentFree: 2399207424
SharedUsed : 9776664, SharedFree : 16437760
```

PID	Process	ResSize	Size
Allocs	Frees	Max	Current
597	clish	3891200	106496
0	0	0	0
631	login	4816896	217088
0	0	0	0
464	ipSecMgr	4587520	274432
367528	0	367528	367528
443	ssMgr	4059136	286720
0	0	0	0
434	ipm	5287936	1208320
330360	0	330360	330360
419	sysd	45555712	30474240
329480	6288190	6255242	6584722
425	sysdlp	17965056	16535552
0	0	0	0
427	sysmon	704512	24576
0	0	0	0
421	sysmon	704512	24576
0	0	0	0
398	flashmnr	843776	36864
0	0	0	0
327	inetd	999424	45056
0	0	0	0
244	sh	860160	2301952
0	0	0	0
74	sh	737280	2301952
0	0	0	0
30	mount_mfs	11755520	2310144
0	0	0	0
25	mount_mfs	167346176	2310144
0	0	0	0
22	mount_mfs	5226496	2310144
0	0	0	0

19	mount_mfs	58314752	2310144
0	0	0	0
12	mount_mfs	520192	2310144
0	0	0	0
2	sh	626688	2301952
0	0	0	0
1	init	233472	2297856
0	0	0	0
0	[system]	97353728	0
0	0	0	0
506	sh	0	0
0	0	0	0
ipc	34060	192	34060 33868
irc	943436	0	943436 943436
RpmAvailMgr	9376	32	9344 9344
ev	133188	0	133188 133188
evterm	26752	0	26752 26752
evhdlr	2528	8064	2528 0
d1m	7556256	7366960	1239104 189296
d1a	416	0	416 416
tsm	15136	0	15136 15136
fmg	766560	0	766560 766560
fileProc	416	0	416 416
sysAdmTsk	42028	0	42028 42028

**Example: show
processes
memory cp**

```
Dell#show processes memory
Total      : 3203928064, MaxUsed      : 804720640 [01/27/2014
06:16:44]
CurrentUsed: 804720640, CurrentFree: 2399207424
SharedUsed : 9776664, SharedFree : 16437760
```

PID	Process	ResSize	Size
Allocs	Frees	Max	Current
597	clish	3891200	106496
0	0	0	0
631	login	4816896	217088
0	0	0	0
464	ipSecMgr	4587520	274432
367528	0	367528	367528
443	ssMgr	4059136	286720
0	0	0	0
434	ipm	5287936	1208320
330360	0	330360	330360
419	sysd	45555712	30474240
329480	6288190	6255242	6584722
425	sysd1p	17965056	16535552
0	0	0	0
427	sysmon	704512	24576
0	0	0	0
421	sysmon	704512	24576
0	0	0	0
398	flashmnt	843776	36864
0	0	0	0
327	inetd	999424	45056
0	0	0	0
244	sh	860160	2301952
0	0	0	0
74	sh	737280	2301952
0	0	0	0
30	mount_mfs	11755520	2310144
0	0	0	0
25	mount_mfs	167346176	2310144
0	0	0	0

```

    22 mount_mfs          5226496      2310144
0      0                  0          0
    19 mount_mfs          58314752     2310144
0      0                  0          0
    12 mount_mfs          520192      2310144
0      0                  0          0
    2  sh                  626688      2301952
0      0                  0          0
    1  init                233472      2297856
0      0                  0          0
    0 [system]            97353728      0
0      0                  0          0
    506 sh                  0          0
0      0                  0          0
ipc      34060             192          34060      33868
irc      943436            0          943436      943436
RpmAvailMgr 9376           32          9344      9344
ev       133188            0          133188     133188
evterm   26752             0          26752     26752
evhdlr   2528              8064         2528      0
dlm      7556256           7366960     1239104     189296
dla      416               0           416       416
tsm      15136             0          15136     15136
fmg      766560            0          766560     766560
fileProc 416               0           416       416
sysAdmTsk 42028            0          42028     42028

```

**Example: show
processes
memory lp all**

Dell#show processes memory lp summary

```

Memory utilization      Total      MaxUsed
CurrentUsed      CurrentFree

```

```

-----
LP2              3203928064      384765952
8456566          3195471498

```

**Example: show
processes
memory lp all**

Dell#show processes memory lp all

Memory Statistics Of Linecard Processor On Slot 2 (bytes)

```

=====
Total: 3203928064, MaxUsed: 386670592, CurrentUsed:
386670592, CurrentFree: 2817257472
TaskName  TotalAllocated      TotalFreed      MaxHeld
CurrentHolding
f10appioserv
163840              147456
      sysdlp
16543744            31641600
      sysmon
24576               704512
      flashmntr
36864               839680
      inetd
45056               995328
      sh
2301952             802816
      sh
2297856             708608
      mount_mfs
2310144            13471744

```

```

    mount_mfs
2310144 52310016
    mount_mfs
2310144 5226496
    mount_mfs
2310144 61145088
    mount_mfs
2310144 503808
    sh
2301952 626688
    init
2297856 233472
    [system]
0 88915968
    tme 433054 0
433054 433054
    ipc 33036 0
33036 33036
    timerMgr 66072 0
66072 66072
    sysAdmTsk 33036 0
33036 33036
    count 33036 0
33036 33036
    tFib4 2016720 0
2016720 2016720
    aclAgent 1490790 0
1490790 1490790
    ifagt_1 202348 0
202348 202348
    dsagt 1325606 0
1325606 1325606
    MacAgent 301474 0
301474 301474
    fib6 1654292 0
1654292 1654292
    ofagt 367522 0
367522 367522
    tnlagt 165180 0
165180 165180
    frrpagt 334400 0
334400 334400

```

**Example: show
processes
memory rp**

Dell#show processes memory rp

```

Total      : 3203928064, MaxUsed      : 376844288 [01/27/2014
06:16:47]
CurrentUsed: 376844288, CurrentFree: 2827083776
SharedUsed : 7993952, SharedFree : 18220472

```

PID	Process	ResSize	Size
Allocs	Frees	Max	Current
496	ofmgr	6000640	573440
896104		896104	896104
392	ndpm	5074944	1052672
301468		301468	301468
160	vrrp	5087232	434176
330360		330360	330360
126	frrp	4640768	282624
301362		301362	301362
154	xstp	8294400	4071424
466654		466654	466654
118	pim	8462336	1372160

3109852	0	3109852	3109852	
434 igmp		5824512	655360	
925008	0	925008	925008	
429 ipml		5255168	921600	
396432	0	396432	396432	
170 mrtm		10838016	6123520	
1127350	0	1127350	1127350	
294 l2mgr		18231296	1347584	
1226308	32948	1226308	1193360	
98 l2pm		4980736	294912	1520714
1120232	433430	400482		
389 arpm		4644864	925696	
301456	0	301456	301456	
367 lacp		5390336	327680	
598792	0	598792	598792	
349 tnlmgr		4554752	131072	
466666	0	466666	466666	
329 otm		4718592	258048	
363396	0	363396	363396	
333 dsm		7159808	2154496	
1094262	0	1094262	1094262	
323 rtm		8933376	1503232	
3109744	0	3109744	3109744	
315 rip		4362240	311296	
198216	0	198216	198216	
309 acl		6483968	1286144	
1259692	0	1259692	1259692	
302 sysd		15392768	3305472	
965786	0	965786	965786	
263 sysmon		704512	24576	
0	0	0	0	
296 flashmnt		839680	36864	
0	0	0	0	
198 inetd		995328	45056	
0	0	0	0	
122 sh		802816	2301952	
0	0	0	0	
74 sh		708608	2297856	
0	0	0	0	
30 mount_mfs		13467648	2310144	
0	0	0	0	
25 mount_mfs		56033280	2310144	
0	0	0	0	

show software ifm

Display interface management (IFM) data.

Z9500

Syntax

```
show software ifm {clients [summary] | ifagt number | ifcb
interface | linecard slot-id | trace-flags}
```

Parameters

clients

Enter the keyword `clients` to display IFM client information.

summary	(OPTIONAL) Enter the keyword <code>summary</code> to display brief information about IFM clients.
ifagt number	Enter the keyword <code>ifagt</code> then the number of an interface agent to display software pipe and IPC statistics.
ifcb interface	Enter the keyword <code>ifcb</code> then one of the following interface IDs then the slot/port information to display interface control block information for that interface: - For a Port Channel interface, enter the keyword <code>port-channel</code> then a number: The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.
trace-flags	Enter the keyword <code>trace-flags</code> to display IFM information for internal trace flags.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.6.1.0	Introduced for the C-Series and S-Series.

Example

```
Dell# show software ifm clients summary
ClntType Inst svcMask subSvcMask tlvSvcMask tlvSubSvc swp
IPM      0 0x00000000 0x00000000 0x90ff71f3 0x021e0e81 31
RTM      0 0x00000000 0x00000000 0x800010ff 0x01930000 43
VRRP     0 0x00000000 0x00000000 0x803330f3 0x00400000 39
L2PM     0 0x00000000 0x00000000 0x87ff79ff 0x0e032200 45
ACL      0 0x00000000 0x00000000 0x867f50c3 0x000f0218 44
OSPF     0 0x00000dfa 0x00400098 0x00000000 0x00000000 0
```

```

PIM      0 0x000000f3 0x00030000 0x00000000 0x00000000 0
IGMP     0 0x000e027f 0x00000000 0x00000000 0x00000000 0
SNMP     0 0x00000000 0x00000000 0x800302c0 0x00000002 30
EVTTERM  0 0x00000000 0x00000000 0x800002c0 0x00000000 29
MRTM     0 0x00000000 0x00000200 0x81f7103f 0x00000000 38
DSM      0 0x00000000 0x00000000 0x80771003 0x00000000 32
LACP     0 0x00000000 0x00000000 0x8000383f 0x00000000 35
DHCP     0 0x00000000 0x00000000 0x800000c2 0x0000c000 37
V6RAD    0 0x00000433 0x00030000 0x00000000 0x00000000 0
Unidentified Client0 0x006e0002 0x00000000 0x00000000
0x00000000 0
Dell#

Dell#show software ifm linecard 0
linecard: 0
          cardType = 516                      numPorts = 144
          numCfgPorts = 0                     cardId =
0x7f0a0a0d
          cardState = 3                      prevHello = 0:0
          notifSeqNum = 1                   ifaNotifSeqNum
= 0 0
          cardAlive = 0                      pStatusMask =
0xffffffff
          ppStatus[0] = 0x00000001          ppStatus[1] =
0x00000001

Dell# show software ifm linecard 0 | find cardstate ignore-case
          cardState = 3                      prevHello = 0:0
          notifSeqNum = 1                   ifaNotifSeqNum
= 0 0
          cardAlive = 0                      pStatusMask =
0xffffffff
          ppStatus[0] = 0x00000001          ppStatus[1] =
0x00000001

Dell# show software ifm linecard 0 | save flash://
sh_sf_ifm_linecard0
Start saving show command report .....

```

show system

Display operational information on all ports or a specified line card.

Z9500

Syntax	show system [brief linecard slot-id]	
Parameters	brief	(OPTIONAL) Enter the keyword brief to view an abbreviated list of system information.
	linecard slot-id	(OPTIONAL) Enter the keyword linecard and a slot number to identify the switch ports. The slot ID range is from 0 to 2.
Command Modes	- EXEC - EXEC Privilege	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	The <code>brief</code> parameter no longer displays the current Reload mode. To display Reload mode, use the <code>show reload-type</code> command. Modified the <code>show system stack-unit</code> command output to support Piece Part ID (PPID).
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	The Boot Flash field displays the code level for boot code 2.8.1.1 and newer, while older boot codes display as "Present".
7.7.1.0	Added Master Priority field.
7.6.1.0	Introduced on the S-Series.

Example

```
Dell#show system brief

System MAC : 74:86:7a:ff:6f:06
Reload-Type: normal-reload [Next boot : normal-reload]

-- Line Card Info --
Linecard UnitType Status ReqTyp CurTyp Version Ports
-----
0 Linecard online Z9500LC36 Z9500LC36 9-5 144
1 Linecard online Z9500LC48 Z9500LC48 9-5 192
2 Linecard online Z9500LC48 Z9500LC48 9-5 192

-- Power Supplies --
Unit Bay Status Type FanStatus FanSpeed(rpm) Power Usage
(W)
-----
0 0 absent
0 1 absent
0 2 absent
0 3 absent

Total power: 0.0 W

-- Fan Status --
Unit Bay TrayStatus Fan0 Speed Fan1 Speed
-----
0 down
1 down
2 down
3 absent
4 down
```

Speed in RPM

Dell#

Related Commands

- [show version](#) – displays the Dell Networking OS version.
- [show hardware](#) – displays the data plane and management plane input and output statistics about a switch component.

show trace

View results of trace operations on the switch or a specified line card.

Z9500

Syntax

```
show trace [linecard slot-id | rp]
```

Parameters

linecard slot-id	Enter the slot ID of the line card for which you want to collect information for tech support. The range of Z9500 slot IDs is from 0 to 2.
rp	Enter the keyword <code>rp</code> to collect information about the Route Processor for tech support.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Example

```
Dell#show trace linecard 2
[9/3 5:18:18] SYS-(tUsrRoot):Spawn TCL Server.
[9/3 5:18:18] SYS-(tUsrRoot):After lpSysInit().
[9/3 5:18:18] SYS-(tUsrRoot):No LONG tick flag defined.
[9/3 5:18:18] SYS-(tUsrRoot):No ULONG tick flag defined.
[9/3 5:18:18] SYS-(tUsrRoot):++TICK_COUNT = 0x0 int: 4, LONG:
4,
[9/3 5:18:33] SYS-(tUsrRoot):Port Pipe Driver Initialized.
Result == ERROR.
[9/3 5:18:33] SYS-(tUsrRoot):Port Pipe Driver prior to Init.
Result == ERROR.
```

```

[9/3 5:18:33] SYS-(tUsrRoot):Binding L2 Loop Back Protocol to
ENDs.
[9/3 5:18:33] SYS-(tUsrRoot):After HWInit().
[9/3 5:18:33] TME-(tme):Var pools for SYS_PART_ID is
initialized
[9/3 5:18:33] TME-(tme):
<<[tme - tme_task2IpBind] - IP Address Added:0x7f0a0a21 -
svce 13 - inst 5>>

[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned ipc svc(14)
inst(5) p_cpid(8)
[9/3 5:18:33] TME-(ipc):f10TaskStartup: svc(14) inst(5)
parentSvc(13) parentInst(5) taskIdx(1812): tskSvc(14)
tskInst(5) p_cpid(8) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned evagt svc(26)
inst(5) p_cpid(9)
[9/3 5:18:33] TME-(evagt):f10TaskStartup: svc(26) inst(5)
parentSvc(13) parentInst(5) taskIdx(3348): tskSvc(26)
tskInst(5) p_cpid(9) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned KP svc(35)
inst(5) p_cpid(10)
[9/3 5:18:33] TME-(KP):f10TaskStartup: svc(35) inst(5)
parentSvc(13) parentInst(5) taskIdx(4500): tskSvc(35)
tskInst(5) p_cpid(10) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned PM svc(34)
inst(5) p_cpid(11)
[9/3 5:18:33] TME-(PM):f10TaskStartup: svc(34) inst(5)
parentSvc(13) parentInst(5) taskIdx(4372): tskSvc(34)
tskInst(5) p_cpid(11) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned timerMgr
svc(45) inst(5) p_cpid(12)
[9/3 5:18:33] TME-(timerMgr):f10TaskStartup: svc(45) inst(5)
parentSvc(13) parentInst(5) taskIdx(5780): tskSvc(45)
tskInst(5) p_cpid(12) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned sysAdmTsk
svc(33) inst(5) p_cpid(13)
[9/3 5:18:33] TME-(sysAdmTsk):f10TaskStartup: svc(33) inst(5)
parentSvc(13) parentInst(5) taskIdx(4244): tskSvc(33)
tskInst(5) p_cpid(13) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] POLLER-(KP):doMasterDetectEvt(): evt has
occurred master slot = 1
[9/3 5:18:33] ***** ERROR TME-(PM):Error:
f10_tmeGetPeerIpAddrByName failed service 30 inst 0

[9/3 5:18:33] TME-(tme):f10TaskCreate: spawned dla svc(32)
inst(5) p_cpid(14)
[9/3 5:18:33] TME-(dla):f10TaskStartup: svc(32) inst(5)
parentSvc(13) parentInst(5) taskIdx(4116): tskSvc(32)
tskInst(5) p_cpid(14) p_procId(302) p_pstate(0x2000d)
[9/3 5:18:33] ***** ERROR TME-(dla):Error:
f10_tmeGetPeerIpAddrByName failed service 253 inst 0

- Repeated 1 time.
----- More -----

```

Related Commands

- [traceroute](#) — displays packet route to a destination device.
-

show tech-support

Display a collection of data from other `show` commands, necessary for Dell Networking technical support to troubleshoot switch operation.

Z9500

Syntax	<code>show tech-support [linecard slot-id page]</code>	
Parameters	linecard slot-id	Enter the slot ID of the line card for which you want to collect information for tech support. The range of Z9500 slot IDs is from 0 to 2. Enter <code>linecard all</code> to collect troubleshooting information on all line cards.
	page	(OPTIONAL) Enter the keyword <code>page</code> to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced <code>save</code> to the file options.
7.6.1.0	Introduced on the S-Series.

Usage Information Without the `page` or `linecard` option, the command output is continuous. To interrupt the command output, use Ctrl-z.

The `save` option works with other filtering commands. This allows you to save specific information of a `show` command. The `save` entry must always be the last option. For example: `Dell#show tech-support |grep regular-expression |except regular-expression | find regular-expression | save flash://result`

This display output is an accumulation of the same information that is displayed when you execute one of the following `show` commands:

- `show cam`

- show clock
- show environment
- show file
- show interfaces
- show inventory
- show ip protocols
- show ip route summary
- show processes cpu
- show processes memory
- show redundancy
- show running-conf
- show version

Example

```
Dell# show tech-support linecard 1

----- show version
-----
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 9-3(0-507)
Copyright (c) 1999-2013 by Dell Inc. All Rights Reserved.
Build Time: Tue Sep 17 15:03:49 PDT 2013
Build Path: /sites/sjc/work/build/buildSpaces/build16/RAINIER-
DEV-9-3-0/SW/SRC
FTOS uptime is 2 hour(s), 26 minute(s)

System image file is "rainier-1-sys"

System Type: Z9500
Control Processor: Intel Centerton with 3203928064 bytes of
memory.

16G bytes of boot flash memory.

  1 144-port TE/FG (SJ)
  2 192-port TE/FG (SJ)
 12 Ten GigabitEthernet/IEEE 802.3 interface(s)

----- show linecard 1 verbose
-----

-- Unit 1 --
Unit Type       : Member Unit
Status          : online
Next Boot       : online
Required Type    : Z9500LC48 - 192-port TE/FG (SJ)
Current Type     : Z9500LC48 - 192-port TE/FG (SJ)
Master priority  : NA
Hardware Rev     : 1.0
Num Ports       : 192
Up Time         : 0 sec
FTOS Version     : 9-3(0-507)
Jumbo Capable    : yes
POE Capable      : no
FIPS Mode        : disabled
Boot Selector    : 3.1.0.1c
Boot Selector    : 3.1.0.1c
Memory Size      : 3203928064 bytes
```



```

Temperature      : 0C
Voltage          : ok
Serial Number    :
Part Number      :                Rev
Vendor Id        :
Date Code        :
Country Code     :
Country Code     :
Piece Part ID    : N/A
PPID Revision    : N/A
Service Tag      : N/A
Expr Svc Code    : N/A
Auto Reboot      : enabled
Burned In MAC    : 74:86:7a:ff:6f:06
No Of MACs       : 3

```

```

----- show environmemt linecard-
voltage -----

```

```
-- linecard Voltage --
```

Slot	Status	1.25V	1.5V	2.5V	3.3V
------	--------	-------	------	------	------

0	ok	0.00V	0.00V	0.00V	0.00V
1	ok	0.00V	0.00V	0.00V	0.00V
2	ok	0.00V	0.00V	0.00V	0.00V

```

----- show process memory on Linecard 1
-----

```

```

Total: 3203928064, MaxUsed: 549421056, CurrentUsed:
549421056, CurrentFree: 2654507008

```

TaskName	TotalAllocated	TotalFreed	MaxHeld
CurrentHolding			
f10appioserv			
163840		147456	
sysdlp			
14929920		54738944	
sysmon			
24576		704512	
flashmntr			
36864		839680	
inetd			
45056		995328	
sh			
2301952		806912	
sh			
2297856		708608	
mount_mfs			
2310144		13484032	
mount_mfs			
2310144		52707328	
mount_mfs			
2310144		5226496	
mount_mfs			
2310144		54476800	
mount_mfs			
2310144		503808	
sh			
2301952		626688	
init			
2297856		233472	
[system]			

0			93728768
	tme	433054	0
433054		433054	
	ipc	33036	0
33036		33036	
	timerMgr	66072	0
66072		66072	
	sysAdmTsk	33036	0
33036		33036	
	count	33036	0
33036		33036	
	tFib4	11472796	0
11472796		11472796	
	aclAgent	1490790	0
1490790		1490790	
	ifagt_1	202348	0
202348		202348	
	dsagt	1325606	0
1325606		1325606	
	fib6	10945628	0
10945628		10945628	
	MacAgent	499162	0
499162		499162	
	ofagt	367522	0
367522		367522	
	tnlagt	165180	0
165180		165180	
	frrpagt	466192	0
466192		466192	
	bfdaTaskMai	202348	0
202348		202348	
Dell (conf) #			

Related Commands

- [show version](#) — displays the Dell Networking OS version.
- [show system](#) — displays the current switch status.
- [show environment](#) — displays the system component status.
-

show util-threshold cpu

Display the utilization thresholds of Z9500 CPUs.

Z9500

Syntax	show util-threshold cpu
Defaults	none
Command Modes	EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series, E-Series, S25 and S50.

Usage Information

Use the `show util-threshold cpu` command to display the CPU utilization thresholds used to send SNMP traps. When Z9500 CPUs exceed the configured time to process packets or data, a threshold notification is sent as an SNMP trap. To reconfigure the currently configured values, use the `util-threshold cpu` command.

Example

```
Dell# show util-threshold cpu
```

Processor	5Sec		1Min		5Min	
	High	Low	High	Low	High	Low
CP	0	0	85	75	80	70
RP	0	0	85	75	80	70
LP 0	0	0	85	75	80	70
LP 1	0	0	85	75	80	70
LP 2	0	0	85	75	80	70

Related Commands

- [util-threshold cpu](#) – Configure CPU utilization thresholds.
- [util-threshold mem](#) – Configure memory utilization thresholds.

show util-threshold memory

Display the memory utilization thresholds of Z9500 CPUs.

Z9500

Syntax `show util-threshold memory`

Defaults None

Command Modes EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series, E-Series, S25 and S50.

Usage Information Use the `show util-threshold memory` command to display the memory utilization thresholds used to send SNMP traps. When Z9500 CPUs exceed the configured (high or low) memory percentage to process packets or data, a threshold notification is sent as an SNMP trap. To reconfigure the currently configured values, use the `util-threshold memory` command.

Example Dell# `show util-threshold memory`

Processor	High	Low
CP	92	82
RP	92	82
LP 0	92	82
LP 1	92	82
LP 2	92	82

Related Commands

- [util-threshold mem](#) – Configure memory utilization thresholds.
- [util-threshold cpu](#) – Configure CPU utilization thresholds.

system location-led

Toggle the location LED of the chassis and (optionally) the location LED of a specified Z9500 port on or off.

Z9500

Syntax `system location-led [interface {fortyGigE | tengigabitethernet} slot/port] {on | off}`

Parameters

<code>interface {fortyGigE tengigabitethernet}</code>	Specify the port type: 40-Gigabit Ethernet or 10-Gigabit Ethernet.
<code>slot / port</code>	Enter the slot and port number. The range of Z9500 slot numbers is 0 to 2.
<code>on off</code>	Turn the location LEDs of the chassis and a specified port on or off.

Defaults The location LEDs of the chassis and Z9500 ports are turned off.

Command Modes EXEC

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.

**Usage
Information**

Use the `system location-led` command to locate the chassis and (optionally) a port on the I/O side of the Z9500 chassis. The location LED setting is not saved through power cycles.

telnet

Connect through Telnet to a server. The Telnet client and server in the Dell Networking OS support IPv4 and IPv6 connections. You can establish a Telnet session directly to the router or a connection can be initiated from the router.

Z9500

Syntax

```
telnet {host | ip-address | ipv6-address prefix-length | vrf  
vrf instance name } [/source-interface]
```

Parameters

host	Enter the name of a server.
ip-address	Enter the IPv4 address in dotted decimal format of the server.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
vrf instance	(Optional) Enter the keyword <code>vrf</code> then the VRF instance name.
source- interface	(OPTIONAL) Enter the keywords <code>/source-interface</code> then the interface information to include the source interface. Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. • For the Null interface, enter the keyword <code>null</code> then 0. • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. • For Tunnel interface types, enter the keyword <code>tunnel</code> then the slot/ port information. The range is from 1 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults	Not configured.																				
Command Modes	- EXEC - EXEC Privilege																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810. Added support for <i>source-interface</i> for link-local IPv6 addressing.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the E-Series ExaScale (IPv6). Increased the number of VLANs on ExaScale to 4094 (was 2094).</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale (IPv4).</td></tr> <tr> <td>7.9.1.0</td><td>Introduced VRF.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series and added support for IPv6 address on the E-Series only.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810. Added support for <i>source-interface</i> for link-local IPv6 addressing.	8.3.11.1	Introduced on the Z9000.	8.2.1.0	Introduced on the E-Series ExaScale (IPv6). Increased the number of VLANs on ExaScale to 4094 (was 2094).	8.1.1.0	Introduced on the E-Series ExaScale (IPv4).	7.9.1.0	Introduced VRF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series and added support for IPv6 address on the E-Series only.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.12.0	Introduced on the S4810. Added support for <i>source-interface</i> for link-local IPv6 addressing.																				
8.3.11.1	Introduced on the Z9000.																				
8.2.1.0	Introduced on the E-Series ExaScale (IPv6). Increased the number of VLANs on ExaScale to 4094 (was 2094).																				
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).																				
7.9.1.0	Introduced VRF.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series and added support for IPv6 address on the E-Series only.																				

terminal length

Configure the number of lines displayed on the terminal screen.

Z9500

Syntax	<code>terminal length <i>screen-length</i></code>	
Parameters	<i>screen-length</i>	Enter a number of lines. Entering zero causes the terminal to display without pausing. The range is from 0 to 512.
Defaults	24 lines	
Command Modes	- EXEC - EXEC Privilege	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

traceroute

View a packet's path to a specific device.

Z9500

Syntax

```
traceroute {host | vrf instance | ip-address | ipv6-address}
```

Parameters

host	Enter the name of device.
vrf instance	(Optional) E-Series Only: Enter the keyword <code>vrf</code> then the VRF Instance name.
ip-address	Enter the IP address of the device in dotted decimal format.
ipv6-address	Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity.



NOTE: The `::` notation specifies successive hexadecimal fields of zeros.

Defaults

- Timeout = **5 seconds**
- Probe count = **3**
- 30 hops max
- 40 byte packet size
- UDP port = **33434**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on the E-Series ExaScale with IPv6.
8.1.1.0	Introduced on the E-Series ExaScale (IPv4 only).
7.9.1.0	Introduced VRF.
7.6.1.0	Added support for the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for IPv6 address on the E-Series.
E-Series	Original command.

Usage Information

When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout (in seconds) (default is **5**), a probe count (default is **3**), minimum TTL (default is **1**), maximum TTL (default is **30**), and port number (default is **33434**). To keep the default setting for those parameters, press the ENTER key.

For IPv6, you are prompted for a minimum hop count (default is **1**) and a maximum hop count (default is **64**).

Example (IPv4)

```
Dell#traceroute www.force10networks.com

Translating "www.force10networks.com"...domain server
(10.11.0.1) [OK]
Type Ctrl-C to abort.

-----
Tracing the route to www.force10networks.com (10.11.84.18),
30 hops max, 40 byte packets
-----

TTL  Hostname                Probe1    Probe2    Probe3
 1   10.11.199.190 001.000 ms 001.000 ms 002.000 ms
 2   gwegress-sjc-02.force10networks.com (10.11.30.126) 005.000
    ms 001.000 ms 001.000 ms
 3   fw-sjc-01.force10networks.com (10.11.127.254) 000.000 ms
    000.000 ms 000.000 ms
 4   www.force10networks.com (10.11.84.18) 000.000 ms 000.000
```



```
ms 000.000 ms
Dell#
```

Example (IPv6)

```
Dell#traceroute 100::1

Type Ctrl-C to abort.

-----
Tracing the route to 100::1, 64 hops max, 60 byte packets
-----
Hops  Hostname  Probe1    Probe2    Probe3
 1      100::1  000.000 ms 000.000 ms 000.000 ms

Dell#traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

-----
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b,
64 hops max, 60 byte packets
-----
Hops  Hostname  Probe1    Probe2    Probe3
 1  3ffe:501:ffff:100:201:e8ff:fe00:4c8b
      000.000 ms 000.000 ms 000.000 ms

Dell#
```

Related Commands

[ping](#) — tests the connectivity to a device.

undebug all

Disable all debug operations on the system.

Z9500

Syntax undebug all

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

upload trace-log

Upload a trace log file from a Z9500 CPU.

Z9500

Syntax	<code>upload trace-log {rp linecard <i>slot-id</i>} {cmd-history hw-trace sw-trace}</code>	
Parameters	rp	Enter the keyword <code>rp</code> to upload a trace log from the Route Processor CPU.
	linecard <i>slot-id</i>	Enter the <code>linecard <i>slot-id</i></code> parameters to specify the line-card CPU whose trace log you want to upload.
	cmd-history	Enter the keyword <code>cmd-history</code> to upload the command history from the specified CPU.
	hw-trace	Enter the keyword <code>hw-trace</code> to upload the hardware trace log from the specified CPU.
	sw-trace	Enter the keyword <code>sw-trace</code> to upload the software trace log from the specified CPU.
Defaults	None.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.5.1.0	Introduced on the C-Series.
Usage Information	Trace log information is uploaded to <code>flash:/TRACE_LOG_DIR</code> .	

util-threshold cpu

Configure the high or low CPU utilization thresholds for SNMP traps.

Z9500

Syntax

```
util-threshold cpu {5sec | 1min | 5min} {cp |rp | linecard  
slot-id | all} {high {0-100} | low {0-100}}
```

Parameters

cpu-utilization-time	Enter one of the following values to configure the threshold level for the time in which a Z9500 CPU can be used: • 5sec • 1min • 5min
cp	Enter the keyword <code>cp</code> to configure the CPU utilization time for the Control Processor CPU.
rp	Enter the keyword <code>rp</code> to configure the CPU utilization time for the Route Processor CPU.
linecard slot-id	Enter the slot ID of the line card for which you want to configure the CPU utilization time. The range of Z9500 slot IDs is from 0 to 2.
all	Enter the keyword <code>all</code> to configure the CPU utilization time on all Z9500 CPUs: Control Processor, Route Processor, and line cards.
{{high low} cpu-utilization-threshold-percentage}	Enter a percentage value to configure the high or low threshold level for the time in which a Z9500 CPU can be used. The percentage of CPU use ranges from 0 to 100.
 NOTE: A threshold level of 0 will disable Syslog and SNMP traps.	

Defaults

- High CPU utilization threshold: 1min = 85%, 5min = 80%
- Low CPU utilization threshold: 1min = 75%, 5min = 70%

Command Modes

CONFIGURATION

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

	Version 8.3.7.0 Description Introduced on the S4810.
Example	<pre>Dell(conf)# util-threshold cpu 5sec cp high 50</pre> In this example, the low threshold value is not specified so it will take the value set for the high threshold value. In all other cases, the low threshold value must be equal to or less than that of the high threshold value.
Usage Information	When the total CPU utilization exceeds the configured threshold for the specified time, a threshold notification is sent as an SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value. The system will generate a Syslog and SNMP trap each time the configured CPU threshold is crossed.  NOTE: The 5sec <code>util-threshold cpu</code> command is disabled by default on all switches. To enable the command, enter <code>util-threshold cpu 5sec all high {value greater than zero}</code>. To disable the Syslog and traps for the 5sec CPU utilization thresholds, enter <code>util-threshold cpu 5sec all high 0</code> or <code>no util-threshold cpu 5sec {cp rp linecard slot-id all}</code>.
Related Commands	• show util-threshold cpu – Display the configured values of CPU utilization thresholds. • show util-threshold memory – Display the configured values of memory utilization thresholds.

util-threshold memory

Configure the high or low memory utilization thresholds for SNMP traps.

Z9500

Syntax	<pre>util-threshold memory {cp rp linecard slot-id all} {[high {0-100}] [low {0-100}]}</pre>	
Parameters	cp Enter the keyword <code>cp</code> to configure the memory utilization threshold for the Control Processor CPU. rp Enter the keyword <code>rp</code> to configure the memory utilization threshold for the Route Processor CPU. linecard slot-id Enter the slot ID of the line card for which you want to configure the memory utilization threshold. The range of Z9500 slot IDs is from 0 to 2. all Enter the keyword <code>all</code> to configure the memory utilization threshold on all Z9500 CPUs: Control Processor, Route Processor, and line cards.	

**{{high | low}
cpu-utilization-
threshold-
percentage}**

Enter a percentage value to configure the high or low threshold level for the percentage of memory a Z9500 CPU can use. The percentage of memory utilization ranges from 0 to 100.



NOTE: A threshold level of 0 will disable Syslog and SNMP traps.

Default

- High threshold: 92%
- Low threshold: 82%

Command Mode

CONFIGURATION

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Example

```
Dell(conf)# util-threshold memory cp high 75 low 67
```

Usage Information

When the total memory utilization for a CPU exceeds the configured high/low threshold for a given time, a threshold notification is sent as a SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value.

To return the memory thresholds to the default values, enter the `no util-threshold mem cp | rp | linecard slot-id | all` command.

Related Commands

- [show util-threshold memory](#) – Display the configured values of memory utilization thresholds.
- [show util-threshold cpu](#) – Display the configured values of CPU utilization thresholds.

virtual-ip

Configure a virtual IP address for the active management interface. You can configure virtual addresses both for IPv4 and IPv6 independently.

Z9500

Syntax

```
virtual-ip {ipv4-address | ipv6-address}
```

To return to the default, use the `no virtual-ip {ipv4-address | ipv6-address}` command.

Parameters

ipv4-address Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.).

ipv6-address Enter an IPv6 address of the active management interface, in the x:x:x:x::x format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

You can configure both IPv4 and IPv6 virtual addresses simultaneously, but only one of each. Each time this command is issued, it replaces the previously configured address of the same family, IPv4 or IPv6. The `no virtual-ip` command takes an address/prefix-length argument, so that the desired address only is removed. If you enter the `no virtual-ip` command without any specified address, then both IPv4 and IPv6 virtual addresses are removed.

Related Commands

[ip address](#) — assigns a primary and secondary IP address to the interface.

write

Copy the current configuration to either the startup-configuration file or the terminal.

Z9500

Syntax	write {memory terminal}																			
Parameters	memory	Enter the keyword <code>memory</code> to copy the current running configuration to the startup configuration file. This command is similar to the <code>copy running-config startup-config</code> command.																		
	terminal	Enter the keyword <code>terminal</code> to copy the current running configuration to the terminal. This command is similar to the <code>show running-config</code> command.																		
Command Modes	EXEC Privilege																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>E-Series</td><td>Original command.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	E-Series	Original command.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.12.0	Introduced on the S4810.																			
8.3.11.1	Introduced on the Z9000.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
E-Series	Original command.																			
Usage Information	The <code>write memory</code> command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named "startup-configuration," the running-config is not saved to that file.																			

802.1X

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only extensible authentication protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking OS supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

The system limits network access for certain users by using virtual local area network (VLAN) assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- If the primary RADIUS server becomes unresponsive, the authenticator begins using a secondary RADIUS server, if configured.
- If no VLAN is supplied by the RADIUS server or if you disable 802.1X authorization, the port configures in its access VLAN after successful authentication.
- If you enable 802.1X authorization but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This safeguard prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If you enable 802.1X authorization and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If you enable port security on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If you disable 802.1X on the port, it returns to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

debug dot1x

Display 802.1X debugging information.

Z9500

Syntax	<code>debug dot1x [all auth-pae-fsm backend-fsm eapol-pdu] [interface <i>interface</i>]</code>	
Parameters	all	Enable all 802.1X debug messages.
	auth-pae-fsm	Enable authentication PAE FSM debug messages.
	backend-fsm	Enable backend FSM debug messages.
	eapol-pdu	Enable the EAPOL frame trace and related debug messages.
	interface <i>interface</i>	Restricts the debugging information to an interface.
Defaults	Disabled	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

Z9500

Syntax	<code>dot1x auth-fail-vlan <i>vlan-id</i> [max-attempts <i>number</i>]</code> To delete the authentication failure VLAN, use the <code>no dot1x auth-fail-vlan <i>vlan-id</i> [max-attempts <i>number</i>]</code> command.
--------	---

Parameters	vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.												
	max-attempts number	(OPTIONAL) Enter the keywords <code>max-attempts</code> followed number of attempts desired before authentication fails. The range is from 1 to 5. The default is 3 .												
Defaults	3 attempts													
Command Modes	CONFIGURATION (<i>conf-if-interface-slot/port</i>)													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.4.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.4.1.0	Introduced on the C-Series and S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.12.0	Introduced on the S4810.													
8.3.11.1	Introduced on the Z9000.													
8.4.1.0	Introduced on the C-Series and S-Series.													
Usage Information	If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface moves to the authentication failed VLAN. After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next reauthentication interval (<code>dot1x reauthentication</code>).													
Related Commands	• dot1x port-control • dot1x guest-vlan • show dot1x interface													

dot1x auth-server

Configure the authentication server to RADIUS.

Z9500

Syntax `dot1x auth-server radius`

Defaults	none														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.12.0	Introduced on the S4810.														
8.3.11.1	Introduced on the Z9000.														
7.6.1.0	Introduced on the C-Series and S-Series.														
7.4.1.0	Introduced on the E-Series.														

dot1x auth-type mab-only

To authenticate a device with MAC authentication bypass (MAB), only use the host MAC address.

Z9500

Syntax	<code>dot1x auth-type mab-only</code>												
Defaults	Disabled												
Command Modes	INTERFACE												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.4.2.1</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.4.2.1	Introduced on the C-Series and S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
8.4.2.1	Introduced on the C-Series and S-Series.												

Usage Information

The prerequisites for enabling MAB-only authentication on a port are:

- Enable 802.1X authentication globally on the switch and on the port (the `dot1x authentication` command).
- Enable MAC authentication bypass on the port (the `dot1x mac-auth-bypass` command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1x authentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the `no dot1x auth-type mab-only` command.

Related Commands

[dot1x mac-auth-bypass](#)

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

Z9500

Syntax

`dot1x authentication`

To disable dot1x on a globally, use the `no dot1x authentication` command.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

dot1x authentication (Interface)

Enable dot1x on an interface. Enable dot1x both globally and at the interface level.

Z9500

Syntax	<code>dot1x authentication</code> To disable dot1x on an interface, use the <code>no dot1x authentication</code> command.
Defaults	Disabled
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

Z9500

Syntax	<code>dot1x guest-vlan <i>vlan-id</i></code> To disable the guest VLAN, use the <code>no dot1x guest-vlan <i>vlan-id</i></code> command.
--------	---

Parameters	vlan-id Enter the VLAN Identifier. The range is from 1 to 4094.												
Defaults	Not configured.												
Command Modes	CONFIGURATION (<i>conf-if-interface-slot/port</i>)												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series, E-Series, and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.												
Usage Information	802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN. If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication, for the device, occurs at the next reauthentication interval (<code>dot1x reauthentication</code>). If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (<code>dot1x auth-fail-vlan</code>).  NOTE: You can create the Layer 3 portion of a guest VLAN and authentication fail VLANs regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.												
Related Commands	• dot1x auth-fail-vlan • dot1x reauthentication • dot1x reauth-max • show dot1x interface												

dot1x host-mode

Enable single-host or multi-host authentication.

Z9500

Syntax	dot1x host-mode {single-host multi-host multi-auth}															
Parameters	single-host	Enable single-host authentication.														
	multi-host	Enable multi-host authentication.														
	multi-auth	Enable multi-supPLICant authentication.														
Defaults	single-host															
Command Modes	INTERFACE															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.4.1.0</td><td>Added the multi-auth option on the C-Series and S-Series.</td></tr><tr><td>8.3.2.0</td><td>Added the single-host and multi-host options on the C-Series, E-Series, and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.4.1.0	Added the multi-auth option on the C-Series and S-Series.	8.3.2.0	Added the single-host and multi-host options on the C-Series, E-Series, and S-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.12.0	Introduced on the S4810.															
8.3.11.1	Introduced on the Z9000.															
8.4.1.0	Added the multi-auth option on the C-Series and S-Series.															
8.3.2.0	Added the single-host and multi-host options on the C-Series, E-Series, and S-Series.															
Usage Information	- Single-host mode authenticates only one host per authenticator port and drops all other traffic on the port. - Multi-host mode authenticates the first host to respond to an Identity Request and then permits all other traffic on the port. - Multi-supPLICant mode authenticates every device attempting to connect to the network on the authenticator port.															
Related Commands	show dot1x interface															

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

Z9500

Syntax	<code>dot1x mac-auth-bypass</code> To disable MAC authentication bypass on a port, use the <code>no dot1x mac-auth-bypass</code> command.
Defaults	Disabled
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

Related Commands	dot1x auth-type mab-only
------------------	--

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

Z9500

Syntax	<code>dot1x max-eap-req number</code> To return to the default, use the <code>no dot1x max-eap-req</code> command.
Parameters	number Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is 2 .

Defaults	2														
Command Modes	INTERFACE														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.12.0	Introduced on the S4810.														
8.3.11.1	Introduced on the Z9000.														
7.6.1.0	Introduced on the C-Series and S-Series.														
7.4.1.0	Introduced on the E-Series.														

dot1x max-suplicants

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in Multi-Auth mode.

Z9500

Syntax	dot1x max-suplicants <i>number</i>							
Parameters	<i>number</i>	Enter the number of supplicants that can be authenticated on a single port in Multi-Auth mode. The range is from 1 to 128. The default is 128 .						
Defaults	128 hosts can be authenticated on a single authenticator port.							
Command Modes	INTERFACE							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

Related
Commands [dot1x host-mode](#)

dot1x port-control

Enable port control on an interface.

Z9500

Syntax	<code>dot1x port-control {force-authorized auto force-unauthorized}</code>						
Parameters	<table> <tr> <td>force-authorized</td><td>Enter the keywords <code>force-authorized</code> to forcibly authorize a port.</td></tr> <tr> <td>auto</td><td>Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.</td></tr> <tr> <td>force-unauthorized</td><td>Enter the keywords <code>force-unauthorized</code> to forcibly deauthorize a port.</td></tr> </table>	force-authorized	Enter the keywords <code>force-authorized</code> to forcibly authorize a port.	auto	Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.	force-unauthorized	Enter the keywords <code>force-unauthorized</code> to forcibly deauthorize a port.
force-authorized	Enter the keywords <code>force-authorized</code> to forcibly authorize a port.						
auto	Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.						
force-unauthorized	Enter the keywords <code>force-unauthorized</code> to forcibly deauthorize a port.						
Defaults	none						
Command Modes	Auto						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.						

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information	The authenticator completes authentication only when <code>port-control</code> is set to <code>auto</code> .
--------------------------	--

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

Z9500

Syntax	<code>dot1x quiet-period seconds</code> To disable quiet time, use the <code>no dot1x quiet-time</code> command.
Parameters	seconds Enter the number of seconds. The range is from 1 to 65535. The default is 60 .
Defaults	60 seconds
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauthentication

Enable periodic reauthentication of the client.

Z9500

Syntax	<code>dot1x reauthentication [interval seconds]</code>
---------------	--

To disable periodic reauthentication, use the `no dot1x reauthentication` command.

Parameters	interval seconds	(Optional) Enter the keyword <code>interval</code> then the interval time, in seconds, after which reauthentication is initiated. The range is from 1 to 31536000 (one year). The default is 3600 (1 hour).
Defaults	3600 seconds (1 hour)	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauth-max

Configure the maximum number of times a port can reauthenticate before the port becomes unauthorized.

Z9500

Syntax	<code>dot1x reauth-max number</code> To return to the default, use the <code>no dot1x reauth-max</code> command.	
Parameters	number	Enter the permitted number of reauthentications. The range is from 1 to 10. The default is 2 .
Defaults	2	
Command Modes	INTERFACE	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

Z9500

Syntax

```
dot1x server-timeout seconds
```

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30 .
----------------	--

Defaults

30 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.6.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description						
7.6.1.0	Introduced on the C-Series and S-Series.						
7.4.1.0	Introduced on the E-Series.						
Usage Information	When you configure the <code>dot1x server-timeout</code> value, take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the <code>dot1x server-timeout</code> value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula: <code>dot1x server-timeout seconds > (radius-server retransmit seconds + 1) * radius-server timeout seconds</code>. Where the default values are as follows: <code>dot1x server-timeout</code> (30 seconds), <code>radius-server retransmit</code> (3 seconds), and <code>radius-server timeout</code> (5 seconds). For example: <pre>Dell(config)#radius-server host 10.11.197.105 timeout 6 Dell(config)#radius-server host 10.11.197.105 retransmit 4 Dell(config)#interface tengigabitethernet 2/23 Dell(config-if-te-2/23)#dot1x server-timeout 40</pre>						

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

Z9500

Syntax	<pre>dot1x supplicant-timeout seconds</pre> To return to the default, use the <code>no dot1x supplicant-timeout</code> command.		
Parameters	<table> <tr> <td>seconds</td><td>Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30.</td></tr> </table>	seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30 .
seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30 .		
Defaults	30 seconds		
Command Modes	INTERFACE		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.		

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x tx-period

Configure the intervals at which EAPOL PDUs the Authenticator PAE transmits.

Z9500

Syntax	<code>dot1x tx-period <i>seconds</i></code> To return to the default, use the <code>no dot1x tx-period</code> command.	
Parameters	seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535. The default is 30 .
Defaults	30 seconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

show dot1x cos-mapping interface

Display the CoS priority-mapping table the RADIUS server provides and applies to authenticated supplicants on an 802.1X-enabled system.

Z9500

Syntax	show dot1x cos-mapping interface <i>interface</i> [mac-address <i>mac-address</i>]													
Parameters	<i>interface</i>	Enter one of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.												
	<i>mac-address</i>	(Optional) MAC address of an 802.1X-authenticated supplicant.												
Defaults	none													
Command Modes	- EXEC - EXEC privilege													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.4.2.1</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.4.2.1	Introduced on the C-Series and S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.12.0	Introduced on the S4810.													
8.3.11.1	Introduced on the Z9000.													
8.4.2.1	Introduced on the C-Series and S-Series.													
Usage Information	Enter a supplicant's MAC address using the <code>mac-address</code> option to display CoS mapping information only for the specified supplicant. You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in Single-Hot, Multi-Host, and Multi-Supplicant authentication modes.													
Example	<pre>Dell#show dot1x cos-mapping interface gigabitethernet 2/21 802.1p CoS re-map table on Gi 2/21:</pre>													


```

-----
Dot1p    Remapped Dot1p
0        7
1        6
2        5
3        4
4        3
5        2
6        1
7        0

Dell#show dot1x cos-mapping int g 2/21 mac-address
00:00:01:00:07:00

802.1p CoS re-map table on Gi 2/21:
-----

802.1p CoS re-map table for Supplicant: 00:00:01:00:07:00
Dot1p    Remapped Dot1p
0        7
1        6
2        5
3        4
4        3
5        2
6        1
7        0

```

show dot1x interface

Display the 802.1X configuration of an interface.

Z9500

Syntax	<code>show dot1x interface <i>interface</i> [mac-address <i>mac-address</i>]</code>	
Parameters	<i>interface</i>	Enter one of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	<i>mac-address</i>	(Optional) MAC address of a supplicant.
Defaults	none	
Command Modes	EXEC	
	EXEC privilege	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added the <code>mac-address</code> option on the C-Series and S-Series.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Usage Information

If you enable 802.1X multi-supplicant authentication on a port, additional 802.1X configuration details (Port Authentication status, Untagged VLAN ID, Authentication PAE state, and Backend state) are displayed for each supplicant, as shown in the following example.

Example

```
Dell#show dot1x int tengig 2/32

802.1x information on Te 2/32:
-----
Dot1x Status:          Enable
Port Control:          AUTO
Port Auth Status:      UNAUTHORIZED
Re-Authentication:     Disable
Untagged VLAN id:      None
Guest VLAN:            Enable
Guest VLAN id:         10
Auth-Fail VLAN:        Enable
Auth-Fail VLAN id:     11
Auth-Fail Max-Attempts: 3
Tx Period:             30 seconds
Quiet Period:          60 seconds
ReAuth Max:            2
Supplicant Timeout:    30 seconds
Server Timeout:        30 seconds
Re-Auth Interval:      3600 seconds
Max-EAP-Req:           2
Auth Type:             SINGLE_HOST
Auth PAE State:        Initialize
Backend State:         Initialize
Dell#
```

Example (mac-address)

```
Dell#show dot1x interface tengig 2/21 mac-address
00:00:01:00:07:00

802.1x information on Te 2/21:
-----
Dot1x Status:          Enable
Port Control:          AUTO
Re-Authentication:     Disable
```

```

Guest VLAN:          Disable
Guest VLAN id:       NONE
Auth-Fail VLAN:      Disable
Auth-Fail VLAN id:   NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:     Enable
Mac-Auth-Bypass Only: Disable
Tx Period:           5 seconds
Quiet Period:        60 seconds
ReAuth Max:          1
Supplicant Timeout:  30 seconds
Server Timeout:      30 seconds
Re-Auth Interval:    60 seconds
Max-EAP-Req:         2
Host Mode:           MULTI_AUTH
Max-Supplicants:     128

```

Port status and State info for Supplicant: 00:00:01:00:07:00

```

Port Auth Status:    AUTHORIZED (MAC-AUTH-BYPASS)
Untagged VLAN id:    4094
Auth PAE State:      Authenticated
Backend State:       Idle
Dell#

```

Example (Interface)

Dell#show dot1x interface tengig 0/21

802.1x information on Te 0/21:

```

-----
Dot1x Status:        Enable
Port Control:        AUTO
Re-Authentication:   Disable
Guest VLAN:          Enable
Guest VLAN id:       100
Auth-Fail VLAN:      Disable
Auth-Fail VLAN id:   NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:     Disable
Mac-Auth-Bypass Only: Disable
Tx Period:           30 seconds
Quiet Period:        60 seconds
ReAuth Max:          3
Supplicant Timeout:  30 seconds
Server Timeout:      30 seconds
Re-Auth Interval:    60 seconds
Max-EAP-Req:         2
Host Mode:           MULTI_AUTH
Max-Supplicants:     128

```

Port status and State info for Supplicant: 00:00:00:00:00:10

```

Port Auth Status:    AUTHORIZED
Untagged VLAN id:    400
Auth PAE State:      Authenticated
Backend State:       Idle

```

Port status and State info for Supplicant: 00:00:00:00:00:11

```

192 | 802.1X
www.dell.com | support.dell.com
Port Auth Status:    AUTHORIZED
Untagged VLAN id:    300
Auth PAE State:      Authenticated
Backend State:       Idle

```

Port status and State info for Supplicant: 00:00:00:00:00:15

Port Auth Status:	AUTHORIZED(GUEST-VLAN)
Untagged VLAN id:	100
Auth PAE State:	Authenticated
Backend State:	Idle

Access Control Lists (ACL)

Access control lists (ACLs) are supported on the Dell Networking operating system on the Z9500 switch. The following types of ACL, IP prefix list, and route maps are supported:

- [Commands Common to all ACL Types](#)
- [Common IP ACL Commands](#)
- [Standard IP ACL Commands](#)
- [Extended IP ACL Commands](#)
- [Standard MAC ACL Commands](#)
- [Extended MAC ACL Commands](#)
- [IP Prefix List Commands](#)
- [Route Map Commands](#)
- [AS-Path Commands](#)
- [IP Community List Commands](#)

 **NOTE:** The number of entries allowed in an ACL is hardware-dependent. For information on the commands to use to re-allocate and display CAM memory space on the Z9500 for Layer 2, IPv4, and IPv6 ACLs, refer to the [Content Addressable Memory \(CAM\)](#) chapter.

 **NOTE:** For ACL commands that use the Trace function, refer to the Trace List Commands section in the [Security](#) chapter.

 **NOTE:** For IPv6 ACL commands, refer to [IPv6 Access Control Lists \(IPv6 ACLs\)](#).

Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands in this chapter may use similar names, but require different options to support the different ACL types (for example, the `deny` and `permit` commands).

remark

Enter a description for an ACL entry.

Z9500

Syntax `remark [remark-number] [description]`

Parameters

remark-number

Enter the remark number. The range is from 0 to 65535.



NOTE: You can use the same sequence number for the remark and an ACL rule.

	<i>description</i> Enter a description of up to 80 characters.																		
Defaults	Not configured.																		
Command Modes	• CONFIGURATION-IP ACCESS LIST-STANDARD • CONFIGURATION-IP ACCESS LIST-EXTENDED • CONFIGURATION-MAC ACCESS LIST-STANDARD • CONFIGURATION-MAC ACCESS LIST-EXTENDED																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.4.1.0	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.4.1.0	Introduced on the E-Series.																		
Usage Information	The <code>remark</code> command is available in each ACL mode. You can configure up to 4294967290 remarks in a given ACL. The following example shows the use of the <code>remark</code> command twice within CONFIGURATION-STANDARD-ACCESS-LIST mode. The same sequence number was used for the remark and for an associated ACL rule. The remark precedes the rule in the running-config because it is assumed that the remark is for the rule with the same sequence number, or the group of rules that follow the remark.																		
Example	<pre> Dell(config-std-nacl)#remark 10 Deny rest of the traffic Dell(config-std-nacl)#remark 5 Permit traffic from XYZ Inc. Dell(config-std-nacl)#show config ! ip access-list standard test remark 5 Permit traffic from XYZ Inc. seq 5 permit 1.1.1.0/24 remark 10 Deny rest of the traffic seq 10 Deny any Dell(config-std-nacl)# </pre>																		
Related Commands	show config — displays the current ACL configuration.																		

show config

Display the current ACL configuration.

Z9500

Syntax `show config`

Command Modes

- CONFIGURATION-IP ACCESS LIST-STANDARD
- CONFIGURATION-IP ACCESS LIST-EXTENDED
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(config-ext-nacl)#show conf
!
ip access-list extended patches
Dell(config-ext-nacl)#
```

Common IP ACL Commands

The following commands are available within both IP ACL modes (Standard and Extended) and do not have mode-specific options. When an ACL is created without a rule and then is applied to an interface, ACL behavior reflects an implicit permit.

The Z9500 supports both Ingress and Egress IP ACLs.



NOTE: Also refer to the [Commands Common to all ACL Types](#) section.

clear counters ip access-group

Erase all counters maintained for access lists.

Z9500

Syntax	<code>clear counters ip access-group [access-list-name]</code>	
Parameters	<i>access-list-name</i>	(OPTIONAL) Enter the name of a configured access-list, up to 140 characters.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

ip access-group

Assign an IP access list (IP ACL) to an interface.

Z9500

Syntax	<code>ip access-group access-list-name {in out} [implicit-permit] [vlan vlan-id]</code> To delete an IP access-group configuration, use the <code>no ip access-group access-list-name {in out} [implicit-permit] [vlan vlan-id]</code> command.
---------------	--

Parameters

<code>access-list-name</code>	Enter the name of a configured access list, up to 140 characters.
<code>in</code>	Enter the keyword <code>in</code> to apply the ACL to incoming traffic.
<code>out</code>	Enter the keyword <code>out</code> to apply the ACL to outgoing traffic.
<code>implicit-permit</code>	(OPTIONAL) Enter the keyword <code>implicit-permit</code> to change the default action of the ACL from <code>implicit-deny</code> to <code>implicit-permit</code> (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
<code>vlan vlan-id</code>	(OPTIONAL) Enter the keyword <code>vlan</code> then the ID numbers of the VLANs. The range is from 1 to 4094 (you can use IDs from 1 to 4094).

Defaults

Not enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

You can assign one ACL (standard or extended ACL) to an interface.



NOTE: This command supports Loopback interfaces EE3 and EF series route processor modules (RPMs). This command does not support Loopback interfaces ED series RPMs, C-Series or S-Series Loopback interfaces.

When you apply an ACL that filters IGMP traffic, all IGMP traffic is redirected to the CPUs and soft-forwarded, if necessary, in the following scenarios:

- on a Layer 2 interface — if a Layer 3 ACL is applied to the interface

- on a Layer 3 port or on a Layer 2/Layer 3 port

Related Commands

[ip access-list standard](#) — configures a standard ACL.

[ip access-list extended](#) — configures an extended ACL.

ip control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv4 CPU traffic.

Z9500

Syntax `ip control-plane egress-filter`

Defaults Not enabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

Z9500

Syntax `show ip accounting {access-list access-list-name | cam_count}
interface interface`

Parameters

access-list-name	Enter the name of the ACL to be displayed.
cam_count	List the count of the CAM rules for this ACL.
interface interface	Enter the keyword <code>interface</code> then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

in | out Identify whether ACL is applied on the ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for the 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Usage Information

<code>show ip accounting access-lists</code> Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	Displays the filter. If the keywords <code>count</code> or <code>byte</code> were configured in the filter, the number of packets or bytes the filter processes is displayed at the end of the line.
"order 4"	Displays the QoS order of priority for the ACL entry.

Example

```
Dell#show ip accounting access FILTER1 interface tengig 1/6
Extended IP access list FILTER1
seq 5 deny ip any 191.1.0.0 /16 count (0x00 packets)
seq 10 deny ip any 191.2.0.0 /16 order 4
seq 15 deny ip any 191.3.0.0 /16
seq 20 deny ip any 191.4.0.0 /16
seq 25 deny ip any 191.5.0.0 /16
```

Standard IP ACL Commands

When you create an ACL without any rule and then apply it to an interface, the ACL behavior reflects an implicit permit.

The Z9500 supports both Ingress and Egress IP ACLs.

 **NOTE:** Also refer to the [Commands Common to all ACL Types](#) and [Common IP ACL Commands](#) sections.

deny

Configure a filter that drops IP packets meeting the filter criteria.

Z9500

Syntax

```
deny {source mask | any | host ip-address} [count [byte] |  
[dscp value] [order] [fragments] [log [interval minutes]  
[threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).

	fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.																						
	log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.																						
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.																						
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.																						
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .																						
Defaults	Not configured.																							
Command Modes	CONFIGURATION-STANDARD-ACCESS-LIST																							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.1.0</td><td>Add the DSCP value for ACL matching.</td></tr><tr><td>8.2.1.0</td><td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Added support for the non-contiguous mask and added the <code>monitor</code> option.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Add the DSCP value for ACL matching.	8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.
Version	Description																							
9.2(1.0)	Introduced on the Z9500.																							
8.3.19.0	Introduced on the S4820T.																							
8.3.11.1	Introduced on the Z9000.																							
8.3.7.0	Introduced on the S4810.																							
8.3.1.0	Add the DSCP value for ACL matching.																							
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.																							
8.1.1.0	Introduced on the E-Series ExaScale.																							
7.6.1.0	Introduced on the S-Series.																							
7.5.1.0	Introduced on the C-Series.																							
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.																							

	Version 6.5.1.0 Description Expanded to include the optional QoS <code>order</code> priority for the ACL entry.
Usage Information	Use the <code>order</code> option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the <i>Z9500 Configuration Guide</i>. When you use the <code>log</code> option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details. By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled. Use the <code>monitor</code> option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the <i>Z9500 Configuration Guide</i>. The software cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.
Related Commands	ip access-list standard — configures a standard ACL. permit — configures a permit filter.

ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

Z9500

Syntax	<pre>ip access-list standard <i>access-list-name</i></pre> To delete an access list, use the <code>no ip access-list standard <i>access-list-name</i></code> command.
Parameters	<i>access-list-name</i> Enter a string up to 140 characters long as the ACL name.
Defaults	All IP access lists contain an implicit "deny any"; that is, if no match occurs, the packet is dropped. ACL permit/deny rules are applied when a packet matches the condition in an entry.
Command Modes	CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.
6.5.1.0	Expanded to include the optional <code>QoS order</code> priority for the ACL entry.

Usage Information

The system supports one ingress and one egress IP ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the Z9500, refer to the Content Addressable Memory (CAM) chapter in the *Z9500 Configuration Guide*.

Example

```
Dell(conf)#ip access-list standard TestList
Dell(config-std-nacl)#
```

Related Commands

[ip access-list extended](#) — creates an extended access list.

[show config](#) — displays the current configuration.

permit

Configure a filter to permit packets from a specific source IP address to be processed and forwarded to another interface on the switch.

Z9500

Syntax

```
permit {source [mask] | any | host ip-address}[count [byte]]
[dscp value] [order] [fragments] [log [interval minutes]
[threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based

Monitoring” section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

Related
Commands

[deny](#) — Assigns a IP ACL filter to deny IP packets.

[ip access-list standard](#) — creates a standard ACL.

resequence access-list

Re-assign sequence numbers to entries in an existing ACL.

Z9500

Syntax

`resequence access-list {ipv4 | ipv6 | mac} {access-list-name StartingSeqNum Step-to-Increment}`

Parameters

**ipv4 | ipv6 |
mac**

Enter the keyword `ipv4`, `ipv6` or `mac` to identify the access-list type to resequence.

**access-list-
name**

Enter the name of a configured ACL.

**StartingSeqNu
m**

Enter the starting sequence number to resequence. For IPv4 and IPv6 ACLs, the range is 0 to 4294967290; for MAC ACLs, the range is 0 to 65535.

**Step-to-
Increment**

Enter the step to increment the sequence number. For IPv4 and IPv6 ACLs, the range is 0 to 4294967290; for MAC ACLs, the range is 0 to 65535.

Defaults

The sequence number of ACL entries increases in multiples of 5; for example, seq 5, seq 10, seq 15 ...

Command
Modes

- EXEC
- EXEC Privilege

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale (IPv6).
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).

	Version	Description
	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing access-list.	
Related Commands	resequence prefix-list ipv4 — resequences a prefix list.	

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

Z9500

Syntax	<code>resequence prefix-list ipv4 {<i>prefix-list-name</i> <i>StartingSeqNum</i> <i>Step-to-increment</i>}</code>	
Parameters	<i>prefix-list-name</i>	Enter the name of the configured prefix list, up to 140 characters long.
	<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. The range is from 0 to 65535.
	<i>Step-to-Increment</i>	Enter the step to increment the sequence number. The range is from 1 to 65535.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale

Version	Description
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands

[resequence access-list](#) — resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

Z9500

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes the filter processes.

dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.

Version	Description
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*. The following conditions apply:

- The `seq sequence-number` command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

Related Commands

[deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward packets.

Extended IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The following commands configure extended IP ACLs, which in addition to the IP address, also examine the packet's protocol type.

The Z9500 supports both Ingress and Egress IP ACLs.

 **NOTE:** Also refer to the [Commands Common to all ACL Types](#) and [Common IP ACL Commands](#) sections.

deny

Configure a filter that drops IP packets meeting the filter criteria.

Z9500

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [bytes]] [dscp value] [order] [monitor] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

ip	Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list denies all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.

count	(OPTIONAL) Enter the keyword <code>count</code> to count packets that the filter processes.
bytes	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Related Commands

[deny tcp](#) — assigns a filter to deny TCP packets.

[deny udp](#) — assigns a filter to deny UDP packets.

[ip access-list extended](#) — creates an extended ACL.

deny icmp

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

Z9500

Syntax

```
deny icmp {source-ip-address mask | any | host ip-address}
{destination mask | any | host ip-address} [log] [dscp] [[count
[bytes]] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.

- Use the `no deny icmp {source-ip-address mask | any | host ip-address} {destination mask | any | host ip-address} command`.

Parameters

source-ip-address	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
dscp	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

Defaults

Not configured.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword <code>dscp</code> .
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

ICMP Message Type Keywords	ICMP Message Type Name
<code>administratively-prohibited</code>	Administratively prohibited
<code>alternate-address</code>	Alternate host address
<code>conversion-error</code>	Datagram conversion error
<code>dod-host-prohibited</code>	Host prohibited
<code>dod-net-prohibited</code>	Net prohibited
<code>echo</code>	Echo
<code>echo-reply</code>	Echo reply

ICMP Message Type Keywords	ICMP Message Type Name
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Network redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Network unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence-unreachable	Precedence cutoff

ICMP Message Type Keywords	ICMP Message Type Name
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects
router-advertisement	Router discovery advertisements
router-solicitation	Router discovery solicitations
source-quench	Source quenches
source-route-failed	Source route failed
time-exceeded	All time exceeded
timestamp-reply	Timestamp replies
timestamp-request	Timestamp requests
traceroute	Traceroute
ttl-exceeded	TTL exceeded
unreachable	All unreachables

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

Z9500

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator
port [port]] {destination mask | any | host ip-address} [dscp]
[bit] [operator port [port]] [count [bytes]] [order]
[fragments] [log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source Enter the IP address of the network or host from which the packets are sent.

<i>mask</i>	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
<i>any</i>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<i>dscp</i>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<i>bit</i>	Enter a flag or combination of bits: • <code>ack</code>: acknowledgement field • <code>fin</code>: finish (no more data from the user) • <code>psh</code>: push function • <code>rst</code>: reset the connection • <code>syn</code>: synchronize sequence numbers • <code>urg</code>: urgent field
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)
<i>port port</i>	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>mask</i>	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
<i>count</i>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.

bytes	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword <code>dscp</code> .

Version	Description
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, `gt`, `lt`, or `range`) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111111000000	7936	7999	64
8	0001111101000000	1111111111111111	8000	8000	1

Total Ports: 4001

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data Mask From To #Covered
1 0000000000000000 1111110000000000 0 1023 1024
Total Ports: 1024
```

Related Commands

[deny](#) — assigns a filter to deny IP traffic.

[deny udp](#) — assigns a filter to deny UDP traffic.

deny udp

To drop user datagram protocol (UDP) packets meeting the filter criteria, configure a filter.

Z9500

Syntax

```
deny udp {source mask | any | host ip-address} [operator port
[port]] {destination mask | any | host ip-address} [dscp]
[operator port [port]] [count [bytes]] [log] [order] [monitor]
[fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
dscp	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)

port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword <code>dscp</code> .
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, `gt`, `lt` or `range`) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111111000000	7936	7999	64
8	0001111101000000	1111111111111111	8000	8000	1

Total Ports: 4001

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000000000000000	1111110000000000	0	1023	1024

Total Ports: 1024

Related Commands

[deny](#) — assigns a filter to deny IP traffic.

[deny tcp](#) — assigns a filter to deny TCP traffic.

ip access-list extended

Configure an extended IP access list (IP ACL) based on IP addresses or protocols.

Z9500

Syntax

```
ip access-list extended access-list-name [cpu-qos]
```

To delete an access list, use the `no ip access-list extended access-list-name [cpu-qos]` command.

Parameters

<i>access-list-name</i>	Enter a string up to 140 characters long as the access list name.
<i>cpu-qos</i>	Enter the keyword <code>cpu-qos</code> to configure an extended IP ACL to be used only to filter protocol traffic for control-plane policing (CoPP).

Defaults

All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

	Version	Description
	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Usage Information	The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the Z9500, refer to the Content Addressable Memory (CAM) chapter in the <i>Z9500 Configuration Guide</i>. If you configure an extended IP ACL to be used only to filter protocol traffic for CoPP, you must enter the keyword <code>cpu-qos</code>.	
Example	<pre>Dell(config)#ip access-list extended TESTListEXTEND Dell(config-ext-nacl)#</pre>	
Related Commands	ip access-list standard — configures a standard IP access list. show config — displays the current configuration.	

permit

To pass IP packets meeting the filter criteria, configure a filter.

Z9500

Syntax	<pre>permit {source mask any host ip-address} {destination mask any host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]]</pre> To remove this filter, you have two choices: - Use the <code>no seq sequence-number</code> command if you know the filter's sequence number. - Use the <code>no deny {source mask any host ip-address} {destination mask any host ip-address}</code> command.	
Parameters	source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
	mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
	any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.

host <i>ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option.
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

The software cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

Related Commands

[ip access-list extended](#) — creates an extended ACL.

[permit tcp](#) — assigns a permit filter for TCP packets.

[permit udp](#) — assigns a permit filter for UDP packets.

permit icmp

Configure a filter to allow all or specific ICMP messages.

Z9500

Syntax

```
permit icmp {source mask | any | host ip-address} {destination  
mask | any | host ip-address} [dscp] [count [bytes]] [order]  
[fragments] [log [interval minutes] [threshold-in-msgs [count]]  
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
host ip-address	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is 0 to 63.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.

	threshold-in-msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .
Defaults	Not configured.	
Command Modes	CONFIGURATION-STANDARD-ACCESS-LIST	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.3.1.0	Added the keyword <code>dscp</code> .
	8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Added support for noncontiguous mask and added the <code>monitor</code> option.
	6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.
Usage Information	Use the <code>order</code> option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the <i>Z9500 Configuration Guide</i>. When you use the <code>log</code> option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details. Use the <code>monitor</code> option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the <i>Z9500 Configuration Guide</i>.	

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to [Port Monitoring](#).



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit tcp

To pass TCP packets meeting the filter criteria, configure a filter.

Z9500

Syntax

```
permit tcp {source mask | any | host ip-address} [bit]
[operator port [port]] {destination mask | any | host ip-
address} [bit] [dscp] [operator port [port]] [count [bytes]]
[log] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • <code>ack</code>: acknowledgement field • <code>fin</code>: finish (no more data from the user) • <code>psh</code>: push function • <code>rst</code>: reset the connection • <code>syn</code>: synchronize sequence numbers • <code>urg</code>: urgent field
dscp	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.

<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the port parameter)
<i>port port</i>	Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>mask</i>	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
<i>count</i>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<i>bytes</i>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<i>log</i>	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
<i>order</i>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
<i>monitor</i>	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .
<i>fragments</i>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

Defaults	Not configured.
Command Modes	CONFIGURATION-EXTENDED-ACCESS-LIST
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword <code>dscp</code> .
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for non-contiguous mask and added the <code>monitor</code> option. Deprecated the keyword <code>established</code> .
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information	Use the <code>order</code> option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the <i>Z9500 Configuration Guide</i>. When you use the <code>log</code> option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details. Use the <code>monitor</code> option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the <i>Z9500 Configuration Guide</i>.
-------------------	---



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, `gt`, `lt`, or `range`) may require more than one entry. The

range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	1111111111111111	8000	8000	1

Total Ports: 4001

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000000000000000	1111110000000000	0	1023	1024

Total Ports: 1024

Related Commands

[ip access-list extended](#) — creates an extended ACL.

[permit](#) — assigns a permit filter for IP packets.

[permit udp](#) — assigns a permit filter for UDP packets.

permit udp

To pass UDP packets meeting the filter criteria, configure a filter.

Z9500

Syntax

```
permit udp {source mask | any | host ip-address} [operator port  
[port]] {destination mask | any | host ip-address} [dscp]  
[operator port [port]] [count [bytes]] [order] [fragments] [log  
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source

Enter the IP address of the network or host from which the packets were sent.

<i>mask</i>	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
<i>any</i>	Enter the keyword <i>any</i> to specify that all routes are subject to the filter.
<i>host ip-address</i>	Enter the keyword <i>host</i> and then enter the IP address to specify a host IP address.
<i>dscp</i>	Enter the keyword <i>dscp</i> to deny a packet based on the DSCP value. The range is from 0 to 63.
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: • <i>eq</i> = equal to • <i>neq</i> = not equal to • <i>gt</i> = greater than • <i>lt</i> = less than • <i>range</i> = inclusive range of ports (you must specify two ports for the <i>port</i> parameter)
<i>port port</i>	Enter the application layer port number. Enter two port numbers if you are using the <i>range</i> logical operand. The range is 0 to 65535.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>count</i>	(OPTIONAL) Enter the keyword <i>count</i> to count packets processed by the filter.
<i>bytes</i>	(OPTIONAL) Enter the keyword <i>bytes</i> to count bytes processed by the filter.
<i>order</i>	(OPTIONAL) Enter the keyword <i>order</i> to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <i>order</i> , the ACLs have the lowest order by default (255).
<i>fragments</i>	Enter the keyword <i>fragments</i> to use ACLs to control packet fragments.
<i>log</i>	(OPTIONAL) Enter the keyword <i>log</i> to include ACL matches in the log.
<i>threshold-in-msgs count</i>	(OPTIONAL) Enter the <i>threshold-in-msgs</i> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <i>seq</i> , <i>permit</i> , or <i>deny</i> commands. The threshold range is from 1 to 100.

	interval <i>minutes</i> (OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes. monitor (OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i>.																								
Defaults	Not configured.																								
Command Modes	CONFIGURATION-EXTENDED-ACCESS-LIST																								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.1.0</td><td>Added the keyword <code>dscp</code>.</td></tr> <tr> <td>8.2.1.0</td><td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Added support for non-contiguous mask and added the <code>monitor</code> option. .</td></tr> <tr> <td>6.5.10</td><td>Expanded to include the optional QoS <code>order</code> priority for the ACL entry.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Added the keyword <code>dscp</code> .	8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	7.4.1.0	Added support for non-contiguous mask and added the <code>monitor</code> option. .	6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.
Version	Description																								
9.2(1.0)	Introduced on the Z9500.																								
8.3.19.0	Introduced on the S4820T.																								
8.3.11.1	Introduced on the Z9000.																								
8.3.7.0	Introduced on the S4810.																								
8.3.1.0	Added the keyword <code>dscp</code> .																								
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.																								
8.1.1.0	Introduced on the E-Series ExaScale.																								
7.6.1.0	Introduced on the S-Series.																								
7.5.1.0	Introduced on the C-Series.																								
7.4.1.0	Added support for non-contiguous mask and added the <code>monitor</code> option. .																								
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.																								
Usage Information	Use the <code>order</code> option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the <i>Z9500 Configuration Guide</i>. When you use the <code>log</code> option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.																								

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, `gt`, `lt`, or `range`) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111000000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	1111111111111111	8000	8000	1

Total Ports: 4001

Example

An ACL rule with a TCP port `lt 1023` uses only one entry in the CAM.

Rule#	Data	Mask	From	To	#Covered
1	0000000000000000	1111110000000000	0	1023	1024

Total Ports: 1024

Related Commands

[ip access-list extended](#) — creates an extended ACL.

[permit](#) — assigns a permit filter for IP packets.

[permit tcp](#) — assigns a permit filter for TCP packets.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

Z9500

Syntax `resequence prefix-list ipv4 {prefix-list-name StartingSeqNum Step-to-increment}`

Parameters

<i>prefix-list-name</i>	Enter the name of the configured prefix list, up to 140 characters long.
<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. The range is from 0 to 65535.
<i>Step-to-Increment</i>	Enter the step to increment the sequence number. The range is from 1 to 65535.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands [resequence access-list](#)— resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

Z9500

Syntax	<pre>seq sequence-number {deny permit} {ip-protocol-number icmp ip tcp udp} {source mask any host ip-address} {destination mask any host ip-address} [operator port [port]] [count [byte] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]</pre>	
Parameters	sequence-number	Enter a number from 0 to 4294967290.
	deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
	permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
	ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
	icmp	Enter the keyword <code>icmp</code> to configure an ICMP access list filter.
	ip	Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list permits all IP protocols.
	tcp	Enter the keyword <code>tcp</code> to configure a TCP access list filter.
	udp	Enter the keyword <code>udp</code> to configure a UDP access list filter.
	source	Enter an IP address in dotted decimal format of the network from which the packet was received.
	mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
	any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	host ip-address	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address or hostname.
	operator	(OPTIONAL) Enter one of the following logical operands: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter.)

<i>port port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>message-type</i>	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.
<i>count</i>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<i>byte</i>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<i>dscp</i>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values. The range is from 0 to 63.
<i>order</i>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
<i>fragments</i>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<i>log</i>	(OPTIONAL) Enter the keyword <code>log</code> to include ACL matches in the log.
<i>threshold-in msgs count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
<i>interval minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
<i>monitor</i>	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based

Monitoring” section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option. Deprecated the keyword <code>established</code> .
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

If you configure the `sequence-number`, the `sequence-number` is used as a tie breaker for rules with the same order.

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *Z9500 Configuration Guide*. The following conditions apply:

- The `seq sequence-number` command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Related
Commands**

[deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward packets.

ACL VLAN Group Commands

Use the commands in this section to configure ACL VLAN groups and CAM optimization for ACLs applied to VLAN groups.

acl-vlan-group

Create an ACL VLAN group.

Term heading	Description heading	
Syntax	<code>acl-vlan-group group name</code>	
	To remove an ACL VLAN group, use the <code>no acl-vlan-group group name</code> command.	
Parameters	group-name	Enter the name of the ACL VLAN group (140 characters maximum).
Default	None	
Command Modes	ACL-VLAN-GROUP CONFIGURATION	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.

Term heading	Description heading
Usage Information	You can configure up to eight different ACL VLAN groups at a time on the switch. When you configure an ACL VLAN group, you enter ACL VLAN Group configuration mode. To avoid the problem of excessive consumption of CAM area, you can configure ACL VLAN groups that combines all the VLANs that are applied with the same ACL in a single group. A unique identifier for each of ACL attached to the VLAN is used as a handle or locator in the CAM area instead of the VLAN id. This method of processing significantly reduces the number of entries in the CAM area and saves memory space in CAM. You can create an ACL VLAN group and attach the ACL with the VLAN members. Optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL maps with the VLAN and increased CAM space utilization occurs. Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

cam-acl-vlan

Configure the number of flow processor (FP) blocks of CAM allocated to ACL VLAN services on the switch.

Syntax	<code>cam-acl-vlan {default vlanopenflow <0-2> vlaniscsi <0-2> vlanaclopt <0-2>}</code>	
Parameters	default	Reset the number of FP blocks to the default value. By default, 0 FP blocks of CAM are allocated for ACL VLAN services, such as iSCSI counters, Open Flow, and ACL VLAN optimization.  NOTE: CAM optimization for ACL VLAN groups is not enabled by default. You must allocate FP blocks of ACL VLAN CAM to enable ACL CAM optimization.
	vlanopenflow <0-2>	Allocate a number FP blocks of CAM for VLAN Open Flow operations.
	vlaniscsi <0-2>	Allocate a number FP blocks of CAM for VLAN iSCSI counters.
	vlanaclopt <0-2>	Allocate a number of FP blocks of CAM for CAM optimization of ACL VLAN operation.
Default	To reset the number FP blocks allocated for ACL VLAN processes, enter the <code>default</code> keyword with the <code>cam-acl-vlan</code> command. By default, 0 FP blocks are allocated for ACL VLAN operations on the switch.	

Command Modes	ACL-VLAN-GROUP CONFIGURATION	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810 and Z9000.
Usage Information	The VLAN ContentAware Processor (VCAP) application is a pre-ingress CAP that modifies the VLAN settings before packets are forwarded. To support the ACL CAM optimization functionality, the CAM carving feature is enhanced. A total of four VACP groups are present, of which two are for fixed groups and the other two are for dynamic groups. Out of the total of two dynamic groups, you can allocate zero, one, or two flow processor (FP) blocks to iSCSI counters, Open Flow and ACL VLAN optimization. You can configure CAM FP blocks for only two of these ACL VLAN services at a time.	

description (ACL VLAN Group)

Add a text description of an ACL VLAN group.

Syntax	<code>description text</code>	
Parameters	<i>description</i>	Enter a text to identify the ACL VLAN group (80 characters maximum).
Default	No default behavior or values	
Command Modes	ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)	
Command History	Version	Description
	9.5(0.0)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.
Usage Information	Enter a description for each ACL VLAN group that you create for effective administrative and logging purposes.	

ip access-group (ACL VLAN Group)

Apply an egress IP ACL to the ACL VLAN group.

Syntax	<code>ip access-group access-list-name out implicit-permit</code>	
Parameters	<i>access-list-name</i>	Enter the name of the egress IP ACL to be applied to member interfaces of the VLAN group (140 characters maximum).
	out	Enter the keyword <code>out</code> to apply the ACL to outgoing traffic.

	implicit-permit	Enter the keyword <code>implicit-permit</code> to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
Default	None	
Command Modes	ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)	
Command History	Version	Description
	9.5(0.0)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.
Usage Information	You can apply only an egress IP ACL on an ACL VLAN group.	

member vlan (ACL VLAN Group)

Add VLAN members to an ACL VLAN group.

Syntax	<code>member vlan {VLAN-range}</code>	
Parameters	VLAN-range	Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8
Default	None	
Command Modes	ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)	
Command History	Version	Description
	9.5(0.0)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.
Usage Information	At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one ACL VLAN group at a time. You can create an ACL VLAN group and attach the ACL with the VLAN members. The optimization is applicable only when you create an ACL VLAN group. If you	

apply an ACL separately on the VLAN interface, each ACL has a mapping with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

show acl-vlan-group

Display the configured ACL VLAN groups on the switch.

Syntax `show acl-vlan-group {group-name | detail}`

Parameters

group-name	Display the configuration of an ACL VLAN group.
detail	Display information about all configured ACL VLAN groups in a line-by-line format.

Default No default behavior or values

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information When an ACL VLAN group name or the access-list name contains more than 30 characters, the name is truncated in the show `show acl-vlan-group group-name` command output.

Examples The following example displays the output of the `show acl-vlan-group` command.



NOTE: Some group names and some access list names are truncated.

```
Dell#show acl-vlan-group
Group Name          Egress IP Acl          Vlan
Members
TestGroupSeventeenTwenty  SpecialAccessOnlyExperts
100,200,300
CustomerNumberIdentifica AnyEmployeeCustomerEleve 2-10,99
HostGroup           Group5                  1,1000
```

The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option.



NOTE: No group or access list names are truncated

```
Dell#show acl-vlan-group detail
```

```

Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300

Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000

```

show cam-acl-vlan

Display the number of FP blocks of CAM that are allocated for different ACL VLAN services, including ACL VLAN optimization, VLAN iSCSI counters, and Open Flow.

Syntax `show cam-acl-vlan`

Command Modes EXEC Privilege

Command History	Version	Description
	9.5(0.0)	Introduced on the Z9500.
	9.3(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information After you allocate FP blocks of CAM to ACL VLAN operation, you must reboot the switch to enable ACL VLAN optimization.

The following table describes the output fields of the `show cam-acl-vlan` command:

Field	Description
Chassis Vlan Cam ACL	Details about the CAM blocks allocated for ACLs for various VLAN operations at a system-wide, global level.
Stack Unit <number>	Details about the CAM blocks allocated for ACLs for various VLAN operations for a particular stack unit.

Field	Description
Current Settings(in block sizes)	Information about the number of FP blocks that are currently in use or allocated.
VlanOpenFlow	Number of FP blocks for VLAN open flow operations.
VlanIscsi	Number of FP blocks for VLAN internet small computer system interface (iSCSI) counters.
VlanHp	Number of FP blocks for VLAN high performance processes.
VlanFcoe	Number of FP blocks for VLAN Fiber Channel over Ethernet (FCoE) operations.
VlanAc1Opt	Number of FP blocks for ACL VLAN optimization feature.

Example

```

Dell#show cam-acl-vlan
-- Chassis Vlan Cam ACL --
      Current Settings(in block sizes)
VlanOpenFlow :      0
VlanIscsi    :      2
VlanHp       :      1
VlanFcoe     :      1
VlanAc1Opt   :      0

-- Stack unit 0 --
      Current Settings(in block sizes)
VlanOpenFlow :      0
VlanIscsi    :      2
VlanHp       :      1
VlanFcoe     :      1
VlanAc1Opt   :      0

```

show cam-usage

Display the amount of memory space used and available in each CAM partition (including Layer 2 ACL, Layer 3 ACL, and IPv4Flow).

Syntax	<code>show cam-usage [acl router switch]</code>	
Parameters	acl	(OPTIONAL) Enter the keyword <code>acl</code> to display Layer 2 and Layer 3 ACL CAM usage.
	router	(OPTIONAL) Enter the keyword <code>router</code> to display Layer 3 CAM usage.

	switch	(OPTIONAL) Enter the keyword <code>switch</code> to display Layer 2 CAM usage.														
Command Modes	- EXEC - EXEC Privilege															
Command History	Version 9.5. (0.0)	Introduced on the Z9500.														
	Version 9.3. (0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.														
Usage Information	The following regions must be provided in the <code>show cam-usage</code> output: - L3AclCam - L2AclCam - V6AclCam The following table describes the output fields of the <code>show cam-usage</code> command. <table><tr><th>Field</th><th>Description</th></tr><tr><td>LineCard</td><td>Number of the line card that contains information on ACL VLAN groups</td></tr><tr><td>Portpipe</td><td>The hardware path that packets follow through a system for ACL optimization</td></tr><tr><td>CAM-Region</td><td>Type of area in the CAM block that is used for ACL VLAN groups</td></tr><tr><td>Total CAM space</td><td>Total amount of space in the CAM block</td></tr><tr><td>Used CAM</td><td>Amount of CAM space that is currently in use</td></tr><tr><td>Available CAM</td><td>Amount of CAM space that is free and remaining to be allocated for ACLs</td></tr></table>		Field	Description	LineCard	Number of the line card that contains information on ACL VLAN groups	Portpipe	The hardware path that packets follow through a system for ACL optimization	CAM-Region	Type of area in the CAM block that is used for ACL VLAN groups	Total CAM space	Total amount of space in the CAM block	Used CAM	Amount of CAM space that is currently in use	Available CAM	Amount of CAM space that is free and remaining to be allocated for ACLs
Field	Description															
LineCard	Number of the line card that contains information on ACL VLAN groups															
Portpipe	The hardware path that packets follow through a system for ACL optimization															
CAM-Region	Type of area in the CAM block that is used for ACL VLAN groups															
Total CAM space	Total amount of space in the CAM block															
Used CAM	Amount of CAM space that is currently in use															
Available CAM	Amount of CAM space that is free and remaining to be allocated for ACLs															

Example 1

```

Dell#show cam-usage
Linecard|Portpipe| CAM Partition | Total CAM | Used CAM
|Available CAM
=====|=====|=====|=====|
1      | 0      | IN-L2 ACL | 1008 | 320
|      | 688    | IN-L2 FIB | 32768 | 1132
|      | 31636  | IN-L3 ACL | 12288 | 2
|      | 12286  | IN-L3 FIB | 262141 | 14
|      | 262127 | IN-L3-SysFlow | 2878 | 45
|      |        |

```

	2833				
		IN-L3-TrcList		1024	0
	1024				
		IN-L3-McastFib		9215	0
	9215				
		IN-L3-Qos		8192	0
	8192				
		IN-L3-PBR		1024	0
	1024				
		IN-V6 ACL		0	0
	0				
		IN-V6 FIB		0	0
	0				
		IN-V6-SysFlow		0	0
	0				
		IN-V6-McastFib		0	0
	0				
		OUT-L2 ACL		1024	0
	1024				
		OUT-L3 ACL		1024	0
	1024				
		OUT-V6 ACL		0	0
	0				
	1	1	IN-L2 ACL	320	0
	320				
		IN-L2 FIB		32768	1136
	31632				
		IN-L3 ACL		12288	2
	12286				
		IN-L3 FIB		262141	14
	262127				
		IN-L3-SysFlow		2878	44
	2834				
	--More--				

Example 2

```
Dell#show cam-usage acl
Linecard|Portpipe| CAM Partition | Total CAM | Used CAM
|Available CAM
=====|=====|=====|=====|=====|
=====|=====|=====|=====|=====|
11 | 0 | IN-L2 ACL | 1008 |
0 | 1008 | IN-L3 ACL | 12288 |
2 | 12286 | OUT-L2 ACL | 1024 |
2 | 1022 | OUT-L3 ACL | 1024 |
0 | 1024
```

Example 3

```
Dell#show cam-usage router
Linecard|Portpipe| CAM Partition | Total CAM | Used CAM
|Available CAM
=====|=====|=====|=====|=====|
=====|=====|=====|=====|=====|
11 | 0 | IN-L3 ACL | 8192 | 3
| 8189 | IN-L3 FIB | 196607 | 1
| 196606 | IN-L3-SysFlow | 2878 | 0
| 2878 | IN-L3-TrcList | 1024 | 0
| 1024
```

				IN-L3-McastFib		9215		0
	9215			IN-L3-Qos		8192		0
	8192			IN-L3-PBR		1024		0
	1024			OUT-L3 ACL		16384		0
	16384			IN-L3 ACL		8192		3
	8189			IN-L3 FIB		196607		1
	196606			IN-L3-SysFlow		2878		0
	2878			IN-L3-TrcList		1024		0
	1024			IN-L3-McastFib		9215		0
	9215			IN-L3-Qos		8192		0
	8192			IN-L3-PBR		1024		0
	1024			OUT-L3 ACL		16384		0
	16384							

Example 4

Dell#show cam-usage switch

Linecard	Portpipe	CAM Partition	Total CAM	Used CAM
Available CAM				
=====	=====	=====	=====	=====
=====	=====	=====	=====	=====
11	0	IN-L2 ACL	7152	0
	7152	IN-L2 FIB	32768	1081
	31687	OUT-L2 ACL	0	0
	0			
11	1	IN-L2 ACL	7152	0
	7152	IN-L2 FIB	32768	1081
	31687	OUT-L2 ACL	0	0
	0			

show running config acl-vlan-group

Display the running configuration of ACL VLAN groups.

Syntax

show running config acl-vlan-group *group-name*

Parameters

group-name

Display the specified ACL VLAN group (140 characters maximum).

Default

None

Command Modes

EXEC

EXEC Privilege

Command History

Version

Description

9.5(0.0)

Introduced on the Z9500.

9.3(0.0)

Introduced on the S4810, S4820T, Z9000 and MXL.

Examples

The following sample output shows the line-by-line style display when using the `show running-config acl-vlan-group` option. Note that no group or access list names are truncated.

```
Dell#show running-config acl-vlan-group
!
acl-vlan-group group1
  description Acl Vlan Group1
  member vlan 1-10,400-410,500
  ip access-group acl1 out implicit-permit
!
acl-vlan-group group2
  member vlan 20
  ip access-group acl2 out
Dell#
```

```
Dell#show running-config acl-vlan-group group1
!
acl-vlan-group group1
  description Acl Vlan Group1
  member vlan 1-10,400-410,500
  ip access-group acl1 out implicit-permit
```

Common MAC ACL Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options. These commands allow you to clear, display, and assign MAC ACL configurations.

The Z9500 supports both Ingress and Egress MAC ACLs.

You can apply a MAC ACL on physical, port-channel and VLAN interfaces. The permit/deny statements in the ACL determine how traffic on an interface, VLAN members, or port-channel members is handled.

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

Z9500

Syntax

```
clear counters mac access-group [mac-list-name]
```

Parameters	<i>mac-list-name</i> (OPTIONAL) Enter the name of a configured MAC access list.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
	The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. You can apply a MAC ACL on a physical, port-channel, or VLAN interface.

Z9500

Syntax	<code>mac access-group <i>access-list-name</i> {in [vlan <i>vlan-range</i>] out}</code> To delete a MAC access-group, use the <code>no mac access-group <i>mac-list-name</i></code> command.
--------	---

Parameters	<i>access-list-name</i>	Enter the name of a configured MAC access list, up to 140 characters.
	<i>vlan vlan-range</i>	(OPTIONAL) Enter the keyword <code>vlan</code> and then enter a range of VLANs. The range is from 1 to 4094 (you can use IDs 1 to 4094).
	 NOTE: This option is available only with the keyword <code>in</code> option.	
	<i>in</i>	Enter the keyword <code>in</code> to configure the ACL to filter incoming traffic.
	<i>out</i>	Enter the keyword <code>out</code> to configure the ACL to filter outgoing traffic.

Defaults	none																				
Command Modes	INTERFACE																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.1.1.0	Introduced on the E-Series.																				
Usage Information	You can assign one ACL (standard or extended) to an interface. If you apply a MAC ACL on a VLAN: • None of the VLAN members can have another ACL applied which has an entry for the VLAN. • The VLAN cannot belong to an ACL VLAN group. If you apply a MAC ACL on a physical or port-channel interface, a VLAN to which the port is associated cannot have another ACL applied. If you apply a MAC ACL on an ACL VLAN group, none of the VLANs in the group can have another ACL applied.																				
Related Commands	mac access-list standard — configures a standard MAC ACL. mac access-list extended — configures an extended MAC ACL.																				

show mac access-lists

Display all of the Layer 2 ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

Z9500

Syntax `show mac access-lists [access-list-name] [interface interface] [in | out]`

Parameters

access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
interface interface	Enter the keyword <code>interface</code> then the one of the following keywords and slot/port or number information: - For a Port Channel interface, enter the keyword <code>port-channel</code> and then enter a number. The C-Series and S-Series range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> and then enter the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> and then enter the slot/port information.
in out	Identify whether ACL is applied on ingress or egress side.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.1.0	Introduced.

show mac accounting access-list

Display MAC access list configurations and counters (if configured).

Z9500

Syntax	<pre>show mac accounting access-list access-list-name interface interface in out</pre>	
Parameters	access-list-name	Enter the name of a configured MAC ACL, up to 140 characters.
	interface interface	Enter the keyword <code>interface</code> then the one of the following keywords and slot/port or number information: - For a Port Channel interface, enter the keyword <code>port-channel</code> and then enter a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> and then enter the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> and then enter the slot/port information.
	in out	Identify whether ACL is applied on ingress or egress side.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series

	Version	Description
	6.1.1.0	Introduced on the E-Series.
Usage Information	The ACL hit counters in this command increment the counters for each matching rule, not just the first matching rule.	
Example	<pre> Dell#show mac accounting access-list mac-ext interface po 1 Extended mac access-list mac-ext on TenGigabitEthernet 0/11 seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19 count (393794576 packets) seq 10 deny host 00:00:00:00:00:21 host 00:00:00:00:00:29 count (89076777 packets) seq 15 deny host 00:00:00:00:00:31 host 00:00:00:00:00:39 count (0 packets) seq 20 deny host 00:00:00:00:00:41 host 00:00:00:00:00:49 count (0 packets) seq 25 permit any any count (0 packets) Extended mac access-list mac-ext on TenGigabitEthernet 0/12 seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19 count (57589834 packets) seq 10 deny host 00:00:00:00:00:21 host 00:00:00:00:00:29 count (393143077 packets) seq 15 deny host 00:00:00:00:00:31 host 00:00:00:00:00:39 count (0 packets) seq 20 deny host 00:00:00:00:00:41 host 00:00:00:00:00:49 count (0 packets) seq 25 permit any any count (0 packets) Dell# </pre>	

Standard MAC ACL Commands

When you create an access control list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. These commands configure standard MAC ACLs.

The Z9500 support both Ingress and Egress MAC ACLs.

 **NOTE:** For more information, also refer to the [Commands Common to all ACL Types](#) and [Common MAC Access List Commands](#) sections.

deny

To drop packets with a matching MAC address, configure a filter.

Z9500

Syntax

```
deny {any | mac-source-address [mac-source-address-mask]}
[count [byte]] [log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.

- Use the `no deny {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
mac-source-address	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of <code>00:00:00:00:00:00</code> is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults

Not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the <code>monitor</code> option.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[permit](#) — configures a MAC address filter to pass packets.

[seq](#) — configures a MAC address filter with a specified sequence number.

mac access-list standard

To configure a standard MAC ACL, name a new or existing MAC access control list (MAC ACL) and enter MAC ACCESS LIST mode. Also refer to the Commands Common to all ACL Types section and the Common MAC Access List Commands section.

Z9500

Syntax

```
mac access-list standard mac-list-name
```

To delete a MAC access list, use the `no mac access-list standard mac-list-name` command.

Parameters

mac-list-name Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults

Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The system supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the Z9500, refer to the Content Addressable Memory (CAM) chapter in the *Z9500 Configuration Guide*.

Example

```
Dell(conf)#mac-access-list access-list standard TestMAC
Dell(config-std-macl)#?
deny          Specify packets to reject
description   List description
exit          Exit from access-list configuration mode
no            Negate a command or set its defaults
permit        Specify packets to forward
remark        Specify access-list entry remark
seq           Sequence numbers
show          Show Standard ACL configuration
```

permit

To forward packets from a specific source MAC address, configure a filter.

Z9500

Syntax

```
permit {any | mac-source-address [mac-source-address-mask]}
[count [byte]] | [log [interval minutes] [threshold-in-msgs
[count]] [monitor]]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword <code>any</code> to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of <code>00:00:00:00:00:00</code> is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[deny](#) — configures a MAC ACL filter to drop packets.

[seq](#) —configure a MAC ACL filter with a specified sequence number.

seq

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

Z9500

Syntax

```
seq sequence-number {deny | permit} {any | mac-source-address
[mac-source-address-mask]} [count [byte]] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, use the `no seq sequence-number` command.

Parameters

sequence-number Enter a number from 0 to 65535.

deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
any	Enter the keyword <code>any</code> to filter all packets.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured

Command Modes CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward packets.

Extended MAC ACL Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit. The following commands configure Extended MAC ACLs.

The Z9500 supports both Ingress and Egress MAC ACLs.



NOTE: For more information, also refer to the [Commands Common to all ACL Types](#) and [Common MAC Access List Commands](#) sections.

deny

To drop packets that match the filter criteria, configure a filter.

Z9500

Syntax

```
deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype-operator] [count  
[byte]] [log [interval minutes] [threshold-in-msgs count]]  
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask}` command.

Parameters

any	Enter the keyword <i>any</i> to drop all packets.
host <i>mac-address</i>	Enter the keyword <i>host</i> and then enter a MAC address to drop packets with that host address.
<i>mac-source-address</i>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<i>mac-source-address-mask</i>	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<i>mac-destination-address</i>	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
<i>mac-destination-address-mask</i>	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • <i>ev2</i> - is the Ethernet II frame format • <i>llc</i> - is the IEEE 802.3 frame format • <i>snap</i> - is the IEEE 802.3 SNAP frame format

count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[permit](#) — configures a MAC address filter to pass packets.

[seq](#) — configures a MAC address filter with a specified sequence number.

mac access-list extended

Configure an extended MAC access control list (extended MAC ACL).

Z9500

Syntax

```
mac access-list extended access-list-name [cpu-qos]
```

To delete a MAC access list, use the `no mac access-list extended access-list-name [cpu-qos]` command.

Parameters

access-list-name

Enter a text string as the MAC access list name, up to 140 characters.

cpu-qos

Enter the keyword `cpu-qos` to configure an extended MAC ACL to be used only to filter protocol traffic for control-plane policing (CoPP).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.

If you configure an extended MAC ACL to be used only to filter protocol traffic for CoPP, you must enter the keyword `cpu-qos`.

Example

```
Dell(conf)#mac-access-list access-list extended TestMATExt
Dell(config-ext-macl)#remark 5 IPv4
Dell(config-ext-macl)#seq 10 permit any any ev2 eq 800 count
bytes
Dell(config-ext-macl)#remark 15 ARP
Dell(config-ext-macl)#seq 20 permit any any ev2 eq 806 count
bytes
Dell(config-ext-macl)#remark 25 IPv6
Dell(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count
bytes
Dell(config-ext-macl)#seq 40 permit any any count bytes
Dell(config-ext-macl)#exit
Dell(conf)#do show mac accounting access-list snickers
interface te 0/47 in
Extended mac access-list snickers on TenGigabitEthernet 0/47
seq 10 permit any any ev2 eq 800 count bytes (559851886
packets 191402152148
bytes)
seq 20 permit any any ev2 eq 806 count bytes (74481486 packets
5031686754
bytes)
seq 30 permit any any ev2 eq 86dd count bytes (7751519 packets
797843521 bytes)
```

Related Commands

[mac access-list standard](#) — configures a standard MAC access list.

[show mac accounting access-list](#) — displays MAC access list configurations and counters (if configured).

permit

To pass packets matching the criteria specified, configure a filter.

Z9500

Syntax

```
permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype operator] [count  
[byte]] | [log [interval minutes] [threshold-in-msgs [count]]]  
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | mac-destination-address mac-destination-address-mask}` command.

Parameters

any	Enter the keyword <i>any</i> to forward all packets.
host	Enter the keyword <i>host</i> then a MAC address to forward packets with that host address.
<i>mac-source-address</i>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<i>mac-source-address-mask</i>	(OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<i>mac-destination-address</i>	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
<i>mac-destination-address-mask</i>	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • <i>ev2</i> - is the Ethernet II frame format • <i>llc</i> - is the IEEE 802.3 frame format • <i>snap</i> - is the IEEE 802.3 SNAP frame format

count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
threshold-in msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[deny](#) — configures a MAC ACL filter to drop packets.

[seq](#) — configure a MAC ACL filter with a specified sequence number.

seq

Configure a filter with a specific sequence number.

Z9500

Syntax

```
seq sequence-number {deny | permit} {any | host mac-address |  
mac-source-address mac-source-address-mask} {any | host mac-  
address | mac-destination-address mac-destination-address-mask}  
[ethertype operator] [count [byte]] [log [interval minutes]  
[threshold-in-msgs [count]]] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number as the filter sequence number. The range is from zero (0) to 65535.
deny	Enter the keyword <code>deny</code> to drop any traffic matching this filter.
permit	Enter the keyword <code>permit</code> to forward any traffic matching this filter.
any	Enter the keyword <code>any</code> to filter all packets.
host mac-address	Enter the keyword <code>host</code> and then enter a MAC address to filter packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.

The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

<i>mac-source-address-mask</i>	Specify which bits in the MAC address must be matched.
<i>mac-destination-address</i>	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
<i>mac-destination-address-mask</i>	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • <code>ev2</code> - is the Ethernet II frame format. • <code>llc</code> - is the IEEE 802.3 frame format. • <code>snap</code> - is the IEEE 802.3 SNAP frame format.
<i>count</i>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<i>byte</i>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<i>log</i>	(OPTIONAL) Enter the keyword <code>log</code> to include ACL messages in the log.
<i>threshold-in-msgs count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
<i>interval minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
<i>monitor</i>	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .

Defaults Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *Z9500 Configuration Guide*.



NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

[deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward packets.

IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.

To configure or enable IP prefix lists, use these commands.

clear ip prefix-list

Reset the number of times traffic meets the conditions ("hit" counters) of the configured prefix lists.

Z9500

Syntax	clear ip prefix-list [<i>prefix-name</i>]																					
Parameters	<i>prefix-name</i>	(OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.																				
Defaults	Clears "hit" counters for all prefix lists unless a prefix list is specified.																					
Command Modes	EXEC Privilege																					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																					
9.2(1.0)	Introduced on the Z9500.																					
8.3.19.0	Introduced on the S4820T.																					
8.3.11.1	Introduced on the Z9000.																					
8.3.7.0	Introduced on the S4810.																					
8.1.1.0	Introduced on the E-Series ExaScale.																					
7.8.1.0	Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.																					
7.6.1.0	Introduced on the S-Series.																					
7.5.1.0	Introduced on the C-Series.																					
6.2.1.1	Introduced on the E-Series.																					
Related Commands	ip prefix-list — configures a prefix list.																					

deny

To drop packets meeting the criteria specified, configure a filter.

Z9500

Syntax	<code>deny ip-prefix [ge min-prefix-length] [le max-prefix-length]</code> To delete a drop filter, use the <code>no deny ip-prefix</code> command.
---------------	---

Parameters	<i>ip-prefix</i>	Specify an IP prefix in the network/length format. For example, 35.0.0.0/ 8 means match the first 8 bits of address 35.0.0.0.
	<i>ge min-prefix-length</i>	(OPTIONAL) Enter the keyword <i>ge</i> and then enter the minimum prefix length, which is a number from zero (0) to 32.
	<i>le max-prefix-length</i>	(OPTIONAL) Enter the keyword <i>le</i> and then enter the maximum prefix length, which is a number from zero (0) to 32.

Defaults Not configured.

Command Modes PREFIX-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the *ge* or *le* options, only packets with an exact match to the prefix are filtered.

Related Commands [permit](#) — configures a filter to pass packets.
[seq](#) — configures a drop or permit filter with a specified sequence number.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

Z9500

Syntax `ip prefix-list prefix-name`
To delete a prefix list, use the `no ip prefix-list prefix-name` command.

Parameters *prefix-name* Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Related Commands [show ip route list](#) — displays IP routes in an IP prefix list.
[show ip prefix-list summary](#) — displays a summary of the configured prefix lists.

permit

Configure a filter that passes packets meeting the criteria specified.

Z9500

Syntax `permit ip-prefix [ge min-prefix-length] [le max-prefix-length]`
To delete a forward filter, use the `no permit ip-prefix` command.

Parameters	ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
	ge min-prefix-length	(OPTIONAL) Enter the keyword <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
	le max-prefix-length	(OPTIONAL) Enter the keyword <code>le</code> and then enter the maximum prefix length, which is a number from zero (0) to 32.

Command Modes PREFIX-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands [deny](#) — configures a filter to drop packets.

[seq](#) — configures a drop or permit filter with a specified sequence number.

seq

To a deny or permit filter in a prefix list while configuring the filter, assign a sequence number.

Z9500

Syntax

```
seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]
```

To delete a specific filter, use the `no seq sequence-number {deny | permit} {any} | [ip-prefix {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]`.

Parameters

sequence-number	Enter a number. The range is from 1 to 65534.
deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition..
permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this condition.
any	(OPTIONAL) Enter the keyword <code>any</code> to match any packets.
ip-prefix /nn	(OPTIONAL) Specify an IP prefix in the network/length format. For example, <code>35.0.0.0/8</code> means match the first 8 bits of address <code>35.0.0.0</code> .
ge min-prefix-length	(OPTIONAL) Enter the keyword <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
le max-prefix-length	(OPTIONAL) Enter the keyword <code>le</code> and then enter the maximum prefix length, which is a number from zero (0) to 32.
bitmask number	Enter the keyword <code>bitmask</code> then enter a bit mask number in dotted decimal format.

Defaults

Not configured.

Command Modes

PREFIX-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the <code>bit mask</code> option.

Usage Information If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands [deny](#) — configures a filter to drop packets.
[permit](#) — configures a filter to pass packets.

show config

Display the current PREFIX-LIST configurations.

Z9500

Syntax `show config`

Command Modes PREFIX-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf-nprefix1)#show config
!
ip prefix-list snickers
Dell(conf-nprefix1)#
```

show ip prefix-list detail

Display details of the configured prefix lists.

Z9500

Syntax	show ip prefix-list detail [<i>prefix-name</i>]	
Parameters	<i>prefix-name</i>	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

Example

```
Dell#show ip prefix-list detail
Prefix-list with the last deletion/insertion: filter_ospf
ip prefix-list filter_in:
count: 3, range entries: 3, sequences: 5 - 10
  seq 5 deny 1.102.0.0/16 le 32 (hit count: 0)
  seq 6 deny 2.1.0.0/16 ge 23 (hit count: 0)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 0)
ip prefix-list filter_ospf:
count: 4, range entries: 1, sequences: 5 - 10
  seq 5 deny 100.100.1.0/24 (hit count: 5)
  seq 6 deny 200.200.1.0/24 (hit count: 1)
```

```

seq 7 deny 200.200.2.0/24 (hit count: 1)
seq 10 permit 0.0.0.0/0 le 32 (hit count: 132)
Dell#

```

show ip prefix-list summary

Display a summary of the configured prefix lists.

Z9500

Syntax	show ip prefix-list summary [<i>prefix-name</i>]	
Parameters	<i>prefix-name</i>	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

Example

```

Dell#show ip prefix summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:

```

```

count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
count: 1, range entries: 1, sequences: 5 - 5
Dell#

```

Route Map Commands

When you create an access-list without any rule and then applied to an interface, the ACL behavior reflects implicit permit.

To configure route maps and their redistribution criteria, use the following commands.

continue

To a route-map entry with a higher sequence number, configure a route-map.

Z9500

Syntax	<code>continue [sequence-number]</code>	
Parameters	<i>sequence-number</i>	(OPTIONAL) Enter the route map sequence number. The range is from 1 to 65535.
Defaults	Not configured.	
Command Modes	ROUTE-MAP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information	The <code>continue</code> feature allows movement from one route-map entry to a specific route-map entry (the sequence number). If you do not specify the sequence number, the <code>continue</code> feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the <code>continue</code> feature
--------------------------	--

executes only after a successful match occurs. If there are no successful matches, the `continue` feature is ignored.

Match clause with Continue clause

The `continue` feature can exist without a match clause. A continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

Set Clause with Continue Clause

If the route-map entry contains sets with the continue clause, set actions are performed first then the continue clause jumps to the specified route map entry.

- If a set action occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same `set` command.
- If `set community additive` and `set as-path prepend` are configured, the communities and AS numbers are prepended.

Related Commands

[set community](#) — specifies a COMMUNITY attribute.

[set as-path](#) — configures a filter to modify the AS path.

description

Add a description to this route map.

Z9500

Syntax

```
description {description}
```

To remove the description, use the `no description {description}` command.

Parameters

description

Enter a description to identify the route map (80 characters maximum).

Defaults

none

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced.

Related Commands [route-map](#) — enables a route map.

match as-path

To match routes that have a certain AS number in their BGP path, configure a filter.

Z9500

Syntax `match as-path as-path-name`
To delete a match AS path filter, use the `no match as-path as-path-name` command.

Parameters ***as-path-name*** Enter the name of an established AS-PATH ACL, up to 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands [set as-path](#) — adds information to the BGP AS_PATH attribute.

match community

To match routes that have a certain COMMUNITY attribute in their BGP path, configure a filter.

Z9500

Syntax `match community community-list-name [exact]`
 To delete a community match filter, use the `no match community` command.

Parameters

<i>community-list-name</i>	Enter the name of a configured community list.
<i>exact</i>	(OPTIONAL) Enter the keywords <code>exact</code> to process only those routes with this community list name.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	Version	Description
	6.1.1.0	Introduced on the E-Series.
Related Commands	ip community-list — configures an Community Access list. set community — specifies a COMMUNITY attribute. neighbor send-community — sends COMMUNITY attribute to peer or peer group.	

match interface

To match routes whose next hop is on the interface specified, configure a filter.

Z9500

Syntax	<code>match interface <i>interface</i></code> To remove a match, use the <code>no match interface <i>interface</i></code> command.	
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: . - For the loopback interface, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. - For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094 (you can use IDs 1 to 4094).
Defaults	Not configured.	
Command Modes	ROUTE-MAP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

[match ip address](#) — redistributes routes that match an IP address.

[match ip next-hop](#) — redistributes routes that match the next-hop IP address.

[match ip route-source](#) — redistributes routes that match routes advertised by other routers.

[match metric](#) — redistributes routes that match a specific metric.

[match route-type](#) — redistributes routes that match a route type.

[match tag](#) — redistributes routes that match a specific tag.

match ip address

To match routes based on IP addresses specified in an access list, configure a filter.

Z9500

Syntax

`match ip address prefix-list-name`

To delete a match, use the `no match ip address prefix-list-name` command.

Parameters

prefix-list-name

Enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

- [match interface](#) — redistributes routes that match the next-hop interface.
- [match ip next-hop](#) — redistributes routes that match the next-hop IP address.
- [match ip route-source](#) — redistributes routes that match routes advertised by other routers.
- [match metric](#) — redistributes routes that match a specific metric.
- [match route-type](#) — redistributes routes that match a route type.
- [match tag](#) — redistributes routes that match a specific tag.

match ip next-hop

To match based on the next-hop IP addresses specified in an IP access list or IP prefix list, configure a filter.

Z9500

Syntax

`match ip next-hop {prefix-list prefix-list-name}`
 To delete a match, use the `no match ip next-hop {prefix-list prefix-list-name}` command.

Parameters

prefix-list
prefix-list-name Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

[match interface](#) — redistributes routes that match the next-hop interface.

[match ip address](#) — redistributes routes that match an IP address.

[match ip route-source](#) — redistributes routes that match routes advertised by other routers.

[match metric](#) — redistributes routes that match a specific metric.

[match route-type](#) — redistributes routes that match a route type.

[match tag](#) — redistributes routes that match a specific tag.

match ip route-source

To match based on the routes advertised by routes specified in IP access lists or IP prefix lists, configure a filter.

Z9500

Syntax

```
match ip route-source {prefix-list prefix-list-name}
```

To delete a match, use the `no match ip route-source {prefix-list prefix-list-name}` command.

Parameters

prefix-list
prefix-list-name

Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults	Not configured.																				
Command Modes	ROUTE-MAP																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.1.1.0	Introduced on the E-Series.																				
Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match metric — redistributes routes that match a specific metric. match route-type — redistributes routes that match a route type. match tag — redistributes routes that match a specific tag.																				

match metric

To match on a specified value, configure a filter.

Z9500

Syntax	<pre>match metric metric-value</pre> To delete a value, use the <code>no match metric [metric-value]</code> command.	
Parameters	metric-value	Enter a value to match. The range is from zero (0) to 4294967295.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match ip route-source — redistributes routes that match routes advertised by other routers. match route-type — redistributes routes that match a route type. match tag — redistributes routes that match a specific tag.
------------------	--

match origin

To match routes based on the value found in the BGP path ORIGIN attribute, configure a filter.

Z9500

Syntax	<pre>match origin {egp igp incomplete}</pre> To disable matching filter, use the <code>no match origin {igp egp incomplete}</code> command.	
Parameters	egp	Enter the keyword <code>egp</code> to match routes originating outside the AS.

	igp	Enter the keyword <code>igp</code> to match routes originating within the same AS.														
	incomplete	Enter the keyword <code>incomplete</code> to match routes with incomplete routing information.														
Defaults	Not configured.															
Command Modes	ROUTE-MAP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking TOS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	6.1.1.0	Introduced on the E-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
8.1.1.0	Introduced on the E-Series ExaScale.															
6.1.1.0	Introduced on the E-Series.															

match route-type

To match routes based on the how the route is defined, configure a filter.

Z9500

Syntax	<pre>match route-type {external [type-1 type-2] internal level-1 level-2 local}</pre> To delete a match, use the <code>no match route-type {local internal external [type-1 type-2] level-1 level-2}</code> command.	
Parameters	external [type-1 type-2]	Enter the keyword <code>external</code> then either <code>type-1</code> or <code>type-2</code> to match only on OSPF Type 1 routes or OSPF Type 2 routes.
	internal	Enter the keyword <code>internal</code> to match only on routes generated within OSPF areas.
	level-1	Enter the keyword <code>level-1</code> to match IS-IS Level 1 routes.
	level-2	Enter the keyword <code>level-2</code> to match IS-IS Level 2 routes.
	local	Enter the keyword <code>local</code> to match only on routes generated within the switch.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match ip route-source — redistributes routes that match routes advertised by other routers. match metric — redistributes routes that match a specific metric. match tag — redistributes routes that match a specific tag.
------------------	---

match tag

To redistribute only routes that match a specified tag value, configure a filter.

Z9500

Syntax	<pre>match tag tag-value</pre> To remove a match, use the <code>no match tag</code> command.
Parameters	tag-value Enter a value as the tag on which to match. The range is from zero (0) to 4294967295.

Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands	match interface — redistributes routes that match the next-hop interface. match ip address — redistributes routes that match an IP address. match ip next-hop — redistributes routes that match the next-hop IP address. match ip route-source — redistributes routes that match routes advertised by other routers. match metric — redistributes routes that match a specific metric. match route-type — redistributes routes that match a route type.
------------------	--

route-map

Enable a route map statement and configure its action and sequence number. This command also places you in ROUTE-MAP mode.

Z9500

Syntax	<pre>route-map map-name [permit deny] [sequence-number]</pre> To delete a route map, use the <code>no route-map map-name [permit deny] [sequence-number]</code> command.
--------	---

Parameters	map-name Enter a text string of up to 140 characters to name the route map for easy identification.
------------	---

	permit (OPTIONAL) Enter the keyword <code>permit</code> to set the route map default as permit. If you do not specify a keyword, the default is <code>permit</code>. deny (OPTIONAL) Enter the keyword <code>deny</code> to set the route map default as deny. sequence-number (OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. The range is from 1 to 65535.																				
Defaults	Not configured. If you do not define a keyword (<code>permit</code> or <code>deny</code>) for the route map, the <code>permit</code> action is the default.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.1.1.0	Introduced on the E-Series.																				
Usage Information	Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same <i>map-name</i> are deleted when you use the <code>no route-map map-name</code> command.																				
Example	<pre>Dell(config)#route-map dempsey Dell(config-route-map)#</pre>																				
Related Commands	show config — displays the current configuration.																				

set as-path

To modify the AS path for border gateway protocol (BGP) routes, configure a filter.

Z9500

Syntax `set as-path prepend as-number [... as-number]`
To remove an AS-Path setting, use the `no set as-path {prepend as-number | tag}` command.

Parameters

prepend as-number	Enter the keyword <code>prepend</code> and then enter up to eight AS numbers to be inserted into the BGP path information. The range is from 1 to 65535.
--------------------------	--

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

Related Commands

- [match as-path](#) — redistributes routes that match an AS-PATH attribute.
- [ip as-path access-list](#) — configures an AS-PATH access list.
- [neighbor filter-list](#) — configures a BGP filter based on the AS-PATH attribute.

[show ip community-lists](#) — displays configured IP Community access lists.

set automatic-tag

To automatically compute the tag value of the route, configure a filter.

Z9500

Syntax	<code>set automatic-tag</code> To return to the default, enter <code>no set automatic-tag</code> .
Defaults	Not configured.
Command Modes	ROUTE-MAP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands	set level — specify the OSPF area for route redistribution. set metric — specify the metric value assigned to redistributed routes. set metric-type — specify the metric type assigned to redistributed routes. set tag — specify the tag assigned to redistributed routes.
-------------------------	--

set comm-list delete

To remove the specified community list from the BGP route's COMMUNITY attribute, configure a filter.

Z9500

Syntax	<pre>set comm-list community-list-name delete</pre> To insert the community list into the COMMUNITY attribute, use the <code>no set comm-list community-list-name delete</code> command.																					
Parameters	community-list-name	Enter the name of an established Community list, up to 140 characters.																				
Defaults	Not configured.																					
Command Modes	ROUTE-MAP																					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																					
9.2(1.0)	Introduced on the Z9500.																					
8.3.19.0	Introduced on the S4820T.																					
8.3.11.1	Introduced on the Z9000.																					
8.3.7.0	Introduced on the S4810.																					
8.1.1.0	Introduced on the E-Series ExaScale.																					
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.																					
7.6.1.0	Introduced on the S-Series.																					
7.5.1.0	Introduced on the C-Series.																					
6.1.1.0	Introduced on the E-Series.																					
Usage Information	The community list used in the <code>set comm-list delete</code> command must be configured so that each filter contains only one community. For example, the filter <code>deny 100:12</code> is acceptable, but the filter <code>deny 120:13 140:33</code> results in an error. If the <code>set comm-list delete</code> command and the <code>set community</code> command are configured in the same route map sequence, the deletion command (<code>set comm-list delete</code>) is processed before the insertion command (<code>set community</code>).																					

Related
Commands

[ip community-list](#) — configures community access list.

[match community](#) — redistributes routes that match the COMMUNITY attribute.

[set community](#) — specifies a COMMUNITY attribute.

set community

Allows you to assign a BGP COMMUNITY attribute.

Z9500

Syntax

```
set community {community-number | local-as | no-advertise | no-export | none} [additive]
```

To delete a BGP COMMUNITY attribute assignment, use the `no set community {community-number | local-as | no-advertise | no-export | none}` command.

Parameters

community-number

Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.

local-AS

Enter the keywords `local-as` to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise

Enter the keywords `no-advertise` to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFF02) community attribute must not be advertised to other BGP peers.

no-export

Enter the keywords `no-export` to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

none

Enter the keyword `none` to remove the community attribute from routes meeting the route map criteria.

additive

(OPTIONAL) Enter the keyword `additive` to add the communities to already existing communities.

Defaults

Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

- [ip community-list](#) — configures community access list.
- [match community](#) — redistributes routes that match the COMMUNITY attribute.
- [neighbor send-community](#) — assigns the COMMUNITY attribute.
- [show ip bgp community](#) — displays BGP community groups.
- [show ip community-lists](#) — displays configured Community access lists.

set level

To specify the IS-IS level or OSPF area to which matched routes are redistributed, configure a filter.

Z9500

Syntax

```
set level {backbone | level-1 | level-1-2 | level-2 | stub-area}
```

To remove a set level condition, use the `no set level {backbone | level-1 | level-1-2 | level-2 | stub-area} command`.

Parameters

backbone	Enter the keyword <code>backbone</code> to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
level-1	Enter the keyword <code>level-1</code> to redistribute matched routes to IS-IS Level 1.

	level-1-2	Enter the keyword <code>level-1-2</code> to redistribute matched routes to IS-IS Level 1 and Level 2.
	level-2	Enter the keyword <code>level-2</code> to redistribute matched routes to IS-IS Level 2.
	stub-area	Enter the keyword <code>stub</code> to redistributed matched routes to OSPF stub areas.
Defaults	Not configured.	
Command Modes	ROUTE-MAP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands	set automatic-tag — computes the tag value of the route.
	set metric — specifies the metric value assigned to redistributed routes.
	set metric-type — specifies the metric type assigned to redistributed routes.
	set tag — specifies the tag assigned to redistributed routes.

set local-preference

To set the BGP LOCAL_PREF attribute for routers within the local autonomous system, configure a filter.

Z9500

Syntax	<code>set local-preference value</code>
	To delete a BGP LOCAL_PREF attribute, use the <code>no set local-preference</code> command.

Parameters	value	Enter a number as the LOCAL_PREF attribute value. The range is from 0 to 4294967295.																		
Defaults	Not configured.																			
Command Modes	ROUTE-MAP																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.0	Introduced on the E-Series.																			
Usage Information	The <code>set local-preference</code> command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the <code>bgp default local-preference</code> command.																			
Related Commands	bgp default local-preference — changes the default LOCAL_PREF attribute for all routes.																			

set metric

To assign a new metric to redistributed routes, configure a filter.

Z9500

Syntax	<pre>set metric [+ -] metric-value</pre> To delete a setting, enter <code>no set metric</code>.	
Parameters	+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
	-	(OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.
	metric-value	Enter a number as the new metric value. The range is from zero (0) to 4294967295.

Defaults	Not configured.																		
Command Modes	ROUTE-MAP																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.1.1.0	Introduced on the E-Series.																		
Related Commands	set automatic-tag — computes the tag value of the route. set level — specifies the OSPF area for route redistribution. set metric-type — specifies the route type assigned to redistributed routes. set tag — specifies the tag assigned to redistributed routes.																		

set metric-type

To assign a new route type for routes redistributed to OSPF, configure a filter.

Z9500

Syntax	<pre>set metric-type {internal external type-1 type-2}</pre> To delete a setting, use the <code>no set metric-type</code> command.	
Parameters	internal	Enter the keyword <code>internal</code> to assign the Interior Gateway Protocol metric of the next hop as the route's BGP MULTI_EXIT_DES (MED) value.
	external	Enter the keyword <code>external</code> to assign the IS-IS external metric.
	type-1	Enter the keyword <code>type-1</code> to assign the OSPF Type 1 metric.
	type-2	Enter the keyword <code>type-2</code> to assign the OSPF Type 2 metric.

Defaults	Not configured.																				
Command Modes	ROUTE-MAP																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.1.0</td><td>Implemented the keyword <code>internal</code>.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Implemented the keyword <code>internal</code> .	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.3.1.0	Implemented the keyword <code>internal</code> .																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.1.1.0	Introduced on the E-Series.																				
Related Commands	set automatic-tag — computes the tag value of the route. set level — specifies the OSPF area for route redistribution. set metric — specifies the metric value assigned to redistributed routes. set tag — specifies the tag assigned to redistributed routes.																				

set next-hop

To specify an IP address as the next hop, configure a filter.

Z9500

Syntax	<pre>set next-hop ip-address</pre> To delete the setting, use the <code>no set next-hop ip-address</code> command.	
Parameters	<i>ip-address</i>	Specify an IP address in dotted decimal format.
Defaults	Not configured.	
Command Modes	ROUTE-MAP	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you configure the `set next-hop` command, its configuration takes precedence over the `neighbor next-hop-self` command in the ROUTER BGP mode.

If you configure the `set next-hop` command with the interface's IP address (either Loopback or physical), the software declares the route unreachable.

Related Commands

[match ip next-hop](#) — redistributes routes that match the next-hop IP address.

set origin

To manipulate the BGP ORIGIN attribute, configure a filter.

Z9500

Syntax

```
set origin {igp | egp | incomplete}
```

To delete an ORIGIN attribute setting, use the `no set origin` command.

Parameters

egp	Enter the keyword <code>egp</code> to set routes originating from outside the local AS.
igp	Enter the keyword <code>igp</code> to set routes originating within the same AS.
incomplete	Enter the keyword <code>incomplete</code> to set routes with incomplete routing information.

Defaults

Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

set tag

To specify a tag for redistributed routes, configure a filter.

Z9500

Syntax `set tag tag-value`
To delete a setting, use the `no set tag` command.

Parameters

tag-value	Enter a number as the tag. The range is from zero (0) to 4294967295.
------------------	--

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

- [set automatic-tag](#) — computes the tag value of the route.
- [set level](#) — specifies the OSPF area for route redistribution.
- [set metric](#) — specifies the metric value assigned to redistributed routes.
- [set metric-type](#) — specifies the route type assigned to redistributed routes.

set weight

To add a non-RFC compliant attribute to the BGP route to assist with route selection, configure a filter.

Z9500

Syntax

```
set weight weight
```

To delete a weight specification, use the `no set weight weight` command.

Parameters

weight Enter a number as the weight used by the route meeting the route map specification. The range is from 0 to 65535. The default is router-originated = **32768** and all other routes = **0**. When there are multiple routes to the same destination, the routes with a higher weight are preferred.

Defaults

router-originated = **32768**; all other routes = **0**

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information If you do not use the `set weight` command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

show config

Display the current route map configuration.

Z9500

Syntax `show config`

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(config-route-map)#show config
!
route-map hopper permit 10
Dell(config-route-map)#
```

show route-map

Display the current route map configurations.

Z9500

Syntax	show route-map [<i>map-name</i>]	
Parameters	<i>map-name</i>	(OPTIONAL) Enter the name of a configured route map, up to 140 characters.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show route-map
route-map firpo, permit, sequence 10
Match clauses:
Set clauses:
tag 34
Dell#
```

Related Commands [route-map](#) — configures a route map.

AS-Path Commands

The following commands configure AS-Path ACLs.

ip as-path access-list

Enter AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

Z9500

Syntax	ip as-path access-list <i>as-path-name</i>																	
Parameters	<i>as-path-name</i>	Enter the access-list name, up to 140 characters.																
Defaults	Not configured.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
8.1.1.0	Introduced on the E-Series ExaScale.																	
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	To apply the AS-PATH ACL to BGP routes, use the <code>match as-path</code> or <code>neighbor filter-list</code> commands.																	
Example	<pre>Dell(conf)#ip as-path access-list TestPath Dell(config-as-path)#</pre>																	
Related Commands	match as-path — matches on routes contain a specific AS-PATH.																	
	neighbor filter-list — configures filter based on AS-PATH information.																	

show ip as-path-access-lists

Display the all AS-PATH access lists configured on the E-Series.

Z9500

Syntax `show ip as-path-access-lists`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip as-path-access-lists
ip as-path access-list 1
  permit ^$
  permit ^\(.*\) $
  deny .*
ip as-path access-list 91
  permit ^$
  deny .*
  permit ^\(.*\) $
Dell#
```

IP Community List Commands

Use the following commands to configure IP community lists on the switch.

ip community-list

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

Z9500

Syntax `ip community-list comm-list-name`
To delete a community-list, use the `no ip community-list comm-list-name` command.

Parameters

<i>comm-list-name</i>	Enter a text string as the name of the community-list, up to 140 characters.
------------------------------	--

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf)#ip community-list TestComList
Dell(config-community-list)#
```

show ip community-lists

Display configured IP community lists in alphabetic order.

Z9500

Syntax `show ip community-lists [name]`

Parameters

<i>name</i>	(OPTIONAL) Enter the name of the standard or extended IP community list, up to 140 characters.
--------------------	--

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

Example

```
Dell#show ip community-lists
ip community-list standard 1
deny 701:20
deny 702:20
deny 703:20
deny 704:20
deny 705:20
deny 14551:20
deny 701:112
deny 702:112
deny 703:112
deny 704:112
deny 705:112
deny 14551:112
deny 701:666
deny 702:666
deny 703:666
deny 704:666
deny 705:666
deny 14551:666
Dell#
```

Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.

The Dell Networking OS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03.

bfd all-neighbors

Enable BFD sessions with all neighbors discovered by Layer 3 protocols virtual router redundancy protocol (VRRP), intermediate system to intermediate system (IS-IS), open shortest path first (OSPF), OSPFv3, or border gateway protocol (BGP) on router interfaces, and (optionally) reconfigure the default timer values.

Z9500

Syntax

```
[vrrp] bfd all-neighbors [interval interval min_rx min_rx
multiplier value role {active | passive}]
```

Parameters

vrrp	Enter the keyword <code>vrrp</code> in INTERFACE mode to enable BFD for VRRP.
interval <i>milliseconds</i>	(OPTIONAL) Enter the keyword <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
min_rx <i>milliseconds</i>	Enter the keyword <code>min_rx</code> to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 100. The default is 100 .
multiplier <i>value</i>	Enter the keyword <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3 .
role [active passive]	Enter the role that the local system assumes: • Active — The active system initiates the BFD session. Both systems can be active for the same session. • Passive — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is active.

Defaults	Refer to <i>Parameters</i> .																						
Command Modes	ROUTER OSPF																						
	ROUTER OSPFv3																						
	ROUTER BGP																						
	ROUTER ISIS																						
	INTERFACE (BFD for VRRP only)																						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2.(0.0)</td><td>Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced BFD for BGP on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced BFD for BGP on the S4810.</td></tr> <tr> <td>8.4.1.3</td><td>Introduced BFD for BGP on the E-Series ExaScale.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced BFD for OSPF and ISIS on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced BFD for OSPF on the C-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced BFD for ISIS on the E-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced BFD for OSPF on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2.(0.0)	Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.	9.0.0.0	Introduced BFD for BGP on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced BFD for BGP on the S4810.	8.4.1.3	Introduced BFD for BGP on the E-Series ExaScale.	8.2.1.0	Introduced BFD for OSPF and ISIS on the E-Series ExaScale.	7.6.1.0	Introduced BFD for OSPF on the C-Series.	7.5.1.0	Introduced BFD for ISIS on the E-Series.	7.4.1.0	Introduced BFD for OSPF on the E-Series.
Version	Description																						
9.2(1.0)	Introduced on the Z9500.																						
9.2.(0.0)	Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.																						
9.0.0.0	Introduced BFD for BGP on the Z9000.																						
8.3.19.0	Introduced on the S4820T.																						
8.3.8.0	Introduced BFD for BGP on the S4810.																						
8.4.1.3	Introduced BFD for BGP on the E-Series ExaScale.																						
8.2.1.0	Introduced BFD for OSPF and ISIS on the E-Series ExaScale.																						
7.6.1.0	Introduced BFD for OSPF on the C-Series.																						
7.5.1.0	Introduced BFD for ISIS on the E-Series.																						
7.4.1.0	Introduced BFD for OSPF on the E-Series.																						
Usage Information	All neighbors inherit the configured timer values except in the following cases: - Timer values configured with the <code>isis bfd all-neighbors</code> or <code>ip ospf bfd all-neighbors</code> commands in INTERFACE mode override timer values configured with the <code>bfd all-neighbors</code> command. Likewise, using the <code>no bfd neighbor</code> command does not disable BFD on an interface if you explicitly enable BFD using the <code>isis bfd all-neighbors</code> command. - Neighbors that have been explicitly enabled or disabled for a BFD session with the <code>bfd neighbor</code> or <code>neighbor bfd disable</code> commands in ROUTER BGP mode do not inherit the global BFD enable/disable values configured with the <code>bfd all-neighbors</code> command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values. You can only enable BFD for VRRP in INTERFACE command mode (<code>vrrp bfd all-neighbors</code>).																						

**Related
Commands**

[show bfd neighbors](#) — displays BFD neighbor information on all interfaces or a specified interface.

[neighbor bfd disable](#) — explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

bfd disable

Disable BFD on an interface.

Z9500

Syntax

`bfd disable`
Re-enable BFD using the `no bfd disable` command.

Defaults

BFD is disabled by default.

**Command
Modes**

VRRP

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on S4810.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

bfd enable (Configuration)

Enable BFD on all interfaces.

Z9500

Syntax	<code>bfd enable</code> Disable BFD using the <code>no bfd enable</code> command.
Defaults	BFD is disabled by default.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

bfd enable (Interface)

Enable BFD on an interface.

Z9500

Syntax	<code>bfd enable</code>
Defaults	BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

bfd interval

Specify non-default BFD session parameters beginning with the transmission interval.

Z9500

Syntax	bfd interval <i>interval</i> min_rx <i>min_rx</i> multiplier <i>value</i> role {active passive}	
Parameters	interval <i>milliseconds</i>	Enter the keywords <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
	min_rx <i>milliseconds</i>	Enter the keywords <code>min_rx</code> to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is 100 .
	multiplier <i>value</i>	Enter the keywords <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3 .
	role [active passive]	Enter the role that the local system assumes: • Active — The active system initiates the BFD session. Both systems can be active for the same session. • Passive — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is Active .
Defaults	Refer to <i>Parameters</i> .	
Command Modes	INTERFACE	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if-te-0/3)#bfd interval 250 min_rx 300 multiplier 4
role passive
Dell(conf-if-te-0/3)#
```

bfd protocol-liveness

Enable the BFD protocol liveness feature.

Z9500

Syntax bfd protocol-liveness

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
7.4.1.0	Introduced on the E-Series.

Usage Information	Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (for example, OSPF and ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.
--------------------------	---

ip route bfd

Enable BFD for all neighbors configured through static routes.

Z9500

Syntax	<code>ip route bfd [interval <i>interval</i> min_rx <i>min_rx</i> multiplier <i>value</i> role {active passive}]</code> To disable BFD for all neighbors configured through static routes, use the <code>no ip route bfd [interval <i>interval</i> min_rx <i>min_rx</i> multiplier <i>value</i> role {active passive}]</code> command.
---------------	---

Parameters	interval <i>milliseconds</i>	(OPTIONAL) Enter the keywords <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
	min_rx <i>milliseconds</i>	Enter the keywords <code>min_rx</code> to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is 100 .
	multiplier <i>value</i>	Enter the keywords <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3 .
	role [active passive]	Enter the role that the local system assumes: • Active — The active system initiates the BFD session. Both systems can be active for the same session. • Passive — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is Active.

Defaults	See Parameters
Command Modes	CONFIGURATION

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	9.2(0.0)	Introduced on Z9000, S4810, and S4820T.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.6.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Related Commands	show bfd neighbors – displays the BFD neighbor information on all interfaces or a specified interface.	

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

Z9500

Syntax	<pre>ipv6 ospf bfd all-neighbors [disable [interval <i>interval</i> min_rx <i>min_rx</i> multiplier <i>value</i> role {active passive}]]</pre> To disable all BFD sessions on an OSPFv3 interface implicitly, use the <code>no ipv6 ospf bfd all-neighbors disable</code> command in interface mode..	
Parameters	disable	(OPTIONAL) Enter the keyword <code>disable</code> to disable BFD on this interface.
	interval <i>milliseconds</i>	(OPTIONAL) Enter the keyword <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
	min_rx <i>milliseconds</i>	Enter the keywords <code>min_rx</code> to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 100. The default is 100 .
	multiplier <i>value</i>	Enter the keyword <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3 .
	role [active passive]	Enter the role that the local system assumes: • Active — The active system initiates the BFD session. Both systems can be active for the same session. • Passive — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

Defaults See Parameters

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.0.0	Introduced on the Z9000, S4820T, and S4810.

Usage Information This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure ipv6 ospf BFD in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword `disable`.

neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

Z9500

Syntax `neighbor {ip-address | peer-group-name} bfd`

Parameters

<i>ip-address</i>	Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
<i>peer-group-name</i>	Enter the name of the peer group that you want to explicitly enable for BFD sessions.

Defaults none

Command Modes ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.
8.4.1.3	Introduced on the E-Series ExaScale.

Usage Information

When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd all-neighbors` command, the default BFD session parameters are used (interval: **100** milliseconds, min_rx: **100** milliseconds, multiplier: **3** packets, and role: **active**) if you have not specified parameters with the `bfd all-neighbors` command.

When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command:

- The neighbor does not inherit the global BFD enable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

Related Commands

[neighbor bfd disable](#) — explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

[show bfd neighbors](#) — displays the BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} bfd disable
```

Parameters

ip-address

Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).

	<i>peer-group-name</i>	Enter the name of the peer group that you want to explicitly disable for BFD sessions.												
Defaults	none													
Command Modes	ROUTER BGP													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.4.1.3</td><td>Introduced on the E-Series ExaScale.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced on the S4810.	8.4.1.3	Introduced on the E-Series ExaScale.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.0.0.0	Introduced on the Z9000.													
8.3.19.0	Introduced on the S4820T.													
8.3.8.0	Introduced on the S4810.													
8.4.1.3	Introduced on the E-Series ExaScale.													
Usage Information	When you explicitly disable a BGP neighbor for a BFD session with the <code>neighbor bfd disable</code> command: • The neighbor does not inherit the global BFD disable values configured with the <code>bfd all-neighbors</code> command or configured for the peer group to which the neighbor belongs. • The neighbor only inherits the global timer values configured with the <code>bfd all-neighbors</code> command: <code>interval</code>, <code>min_rx</code>, and <code>multiplier</code>. When you remove the Disabled state of a BFD for a BGP session with a specified neighbor by entering the <code>no neighbor bfd disable</code> command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the <code>bfd all-neighbors</code> command or configured for the peer group to which the neighbor belongs.													
Related Commands	show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.													

show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

Z9500

Syntax	<code>show bfd neighbors interface [detail]</code>	
Parameters	interface	Enter one of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information. - For a port-channel interface, enter the keyword <code>port-channel</code> then a number. For the C-Series, Z-Series, and S8410, the range is from 1 to 128. - For VLAN interfaces, enter the keyword <code>vlan</code> then a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1 to 2730 (VLAN IDs can be from 0 to 4093).
	detail	(OPTIONAL) Enter the keyword <code>detail</code> to view detailed information about BFD neighbors.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Added support for BFD for BGP on the S4810.
8.4.1.3	Added support for BFD for BGP on the E-Series ExaScale.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Added support for BFD for VLAN and port-channel interfaces on the E-Series.
7.4.1.0	Introduced BFD on physical ports on the E-Series.

Example

```
Dell#show bfd neighbors

*      - Active session role
Ad Dn - Admin Down
B      - BGP
C      - CLI
I      - ISIS
O      - OSPF
R      - Static Route (RTM)

  LocalAddr  RemoteAddr  Interface  State  Rx-int  Tx-int  Mult
Clients
* 10.1.3.2   10.1.3.1     Te 1/3    Up     300    250    3    C
```

Example (Detail)

```
Dell#show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: TenGigabitEthernet 1/3
State: Up
Configured parameters:
  TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
  TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
  TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
  Number of packets received from neighbor: 376
  Number of packets sent to neighbor: 314
  Number of state changes: 2
  Number of messages from IFA about port state change: 0
  Number of messages communicated b/w Manager and Agent: 6
Dell#
```

Related Commands

[bfd all-neighbors](#) — establishes BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

vrrp bfd

Establish a BFD session with VRRP neighbors.

Z9500

Syntax

```
vrrp bfd {all-neighbors | neighbor ip-address} [interval  
interval min_rx min_rx multiplier value role {active |  
passive}]
```

To undo your VRRP BFD configuration, use the `no vrrp bfd {all-neighbors | neighbor ip-address } [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

Parameters

all-neighbors	Establish BFD sessions with all BFD neighbors on an interface.
neighbor ip-address	Enter the IP address of the BFD neighbor.
interval milliseconds	(OPTIONAL) Enter the keyword <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is 50 to 1000. The default is 100 .
min_rx milliseconds	Enter the keyword <code>min_rx</code> to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is 50 to 1000. The default is 100 .
multiplier	Enter the keyword <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is 3 to 50. The default is 3 .
role [active passive]	Enter the role that the local system assumes: • Active—The active system initiates the BFD session. Both systems can be active for the same session. • Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is Active.

Defaults

See Parameters.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

When BFD is enabled with VRRP neighbors, the VRRP protocol registers with the BFD manager on the route processor. BFD sessions are established with all neighboring interfaces participating in VRRP. If a neighboring interface fails, the BFD agent on the line card notifies the BFD manager, which in turn notifies the VRRP protocol that a link state change occurred.

Border Gateway Protocol

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless inter-domain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically sent messages to update those routing tables.

BGP is supported in Dell Networking OS version 9.0.0.0 for the Z9000 platform Dell Networking OS version 8.3.7.0 for the S4810 platform Dell Networking OS version 8.3.19.0 for the S4820T platform Dell Networking OS version 9.0.2.0 for the S6000 platform



NOTE: For more information about configuring the border gateway protocol (BGP), refer to the BGP chapter in the *Dell Networking OS Configuration Guide*.

This chapter contains the following sections:

- BGPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)
- IPv6 BGP Commands

BGP IPv4 Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP supports classless interdomain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

address-family

Enable the IPv4 multicast or the IPv6 address family.

Z9500

Syntax	<code>address-family [ipv4 multicast ipv6unicast]</code>	
Parameters	ipv4 multicast	Enter BGPv4 multicast mode.
	ipv6 unicast	Enter BGPv6 mode.
Defaults	Not configured.	
Command Modes	ROUTER BGP	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.5.1.0	Introduced

aggregate-address

To minimize the number of entries in the routing table, summarize a range of prefixes.

Z9500

Syntax

```
aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]
```

Parameters

<i>ip-address</i> <i>mask</i>	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
<i>advertise-map</i> <i>map-name</i>	(OPTIONAL) Enter the keywords <i>advertise-map</i> then the name of a configured route map to set filters for advertising an aggregate route.
<i>as-set</i>	(OPTIONAL) Enter the keyword <i>as-set</i> to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
<i>attribute-map</i> <i>map-name</i>	(OPTIONAL) Enter the keywords <i>attribute-map</i> then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
<i>summary-only</i>	(OPTIONAL) Enter the keyword <i>summary-only</i> to advertise only the aggregate address. Specific routes are not advertised.
<i>suppress-map</i> <i>map-name</i>	(OPTIONAL) Enter the keywords <i>suppress-map</i> then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults	Not configured.														
Command Modes	- ROUTER BGP ADDRESS FAMILY - ROUTER BGP ADDRESS FAMILY IPv6														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active. If routes within the aggregate are constantly changing, do not add the <code>as-set</code> parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH. In route maps used in the <code>suppress-map</code> parameter, routes meeting the <code>deny</code> clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the <code>permit</code> clause are suppressed. If the route is injected via the <code>network</code> command, that route still appears in the routing table if the <code>summary-only</code> parameter is configured in the <code>aggregate-address</code> command. The <code>summary-only</code> parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the <code>neighbor distribute-list</code> command. In the <code>show ip bgp</code> command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.														

Defaults	Disabled (that is, the software only compares MEDs from neighbors within the same AS).														
Command Modes	ROUTER BGP														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced command.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced command.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.2.1.0	Introduced command.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	Any update without a MED attribute is the least preferred route. If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.														

bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

Z9500

Syntax	<pre>bgp asnotation [asplain asdot+ asdot]</pre> To disable a dot or dot+ representation and return to ASPLAIN, enter the <code>no bgp asnotation</code> command.				
Defaults	asplain				
Command Modes	ROUTER BGP				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the dynamic application of AS notation changes
8.2.1.0	Introduced

Usage Information

Before enabling this feature, enable the `enable bgp four-octet-as-support` command. If you disable the `four-octet-support` command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation shows.

Example

```
Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asdot
Dell(conf-router_bgp)#ex
Dell(conf)#do show run | grep bgp

router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot

Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asdot+
Dell(conf-router_bgp)#ex

Dell(conf)#do show run | grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot+

Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asplain
Dell(conf-router_bgp)#ex
Dell(conf)#do show run |grep bgp
router bgp 1
  bgp four-octet-as-support

Dell(conf)#
```

Related Commands

[bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

Z9500

Syntax `bgp bestpath as-path ignore`

To return to the default, enter the `no bgp bestpath as-path ignore` command.

Defaults Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path multipath-relax

Include prefixes received from different AS paths during multipath calculation.

Z9500

Syntax `bgp bestpath as-path multipath-relax`
To return to the default BGP routing process, use the `no bgp bestpath as-path multipath-relax` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

	Version	Description
	8.3.19.0	Introduced on the S4820T.
	8.3.11.4	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
Usage Information	The <code>bestpath router bgp configuration mode</code> command changes the default bestpath selection algorithm. The <code>multipath-relax</code> option allows load-sharing across providers with different (but equal-length) autonomous system paths. Without this option, ECMP expects the AS paths to be identical for load-sharing.	

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Z9500

Syntax	<code>bgp bestpath med confed</code> To disable MED comparison on BGP confederation paths, enter the <code>no bgp bestpath med confed</code> command.
Defaults	Disabled
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Introduced on the S-Series.
	7.7.1.0	Introduced on the C-Series.
Usage Information	The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.	

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over paths with an advertised MED attribute.

Z9500

Syntax `bgp bestpath med missing-as-best`
To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
6.3.1.0	Introduced

Usage Information The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over paths with a higher MED.

bgp bestpath router-id ignore

Do not compare router-id information for external paths during best path selection.

Z9500

Syntax `bgp bestpath router-id ignore`
To return to the default selection, use the `no bgp bestpath router-id ignore` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced

Usage Information Configuring this option retains the current best-path. When sessions are then reset, the oldest received path is chosen as the best-path.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

Z9500

Syntax `bgp client-to-client reflection`
To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.

Defaults Enabled when a route reflector is configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	Route reflection to clients is not necessary if all client routers are fully meshed.
Related Commands	bgp cluster-id — assigns an ID to a BGP cluster with two or more route reflectors. neighbor route-reflector-client — configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Z9500

Syntax	<pre>bgp cluster-id {ip-address number}</pre> To delete a cluster ID, use the <code>no bgp cluster-id {ip-address number}</code> command.
--------	--

Parameters	ip-address	Enter an IP address as the route reflector cluster ID.
	number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults	Not configured.
----------	-----------------

Command Modes	ROUTER BGP
---------------	------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the <code>bgp cluster-id</code> command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.
-------------------	---

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

**Related
Commands**

[bgp client-to-client reflection](#) — enables route reflection between the route reflector and clients.

[neighbor route-reflector-client](#) — configures a route reflector and clients.

[show ip bgp cluster-list](#) — views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

Z9500

Syntax

`bgp confederation identifier as-number`

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number

Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults

Not configured.

**Command
Modes**

ROUTER BGP

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added support for the 4-byte format

**Usage
Information**

To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGp neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGp peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

Related Commands [bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

Z9500

Syntax	<code>bgp confederation peers as-number [...as-number]</code>	
	To return to the default, use the <code>no bgp confederation peers</code> command.	
Parameters	as-number	Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
	...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added support for the 4-byte format.

Usage Information

All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGp neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

This command automatically restarts the BGP instance for the configuration to take effect.

Related Commands

[bgp confederation identifier](#) — configures a confederation ID.

[bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

Z9500

Syntax

```
bgp dampening [half-life reuse suppress max-suppress-time]  
[route-map map-name]
```

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

<i>half-life</i>	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is from 1 to 45. The default is 15 minutes .
<i>reuse</i>	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is 750 .
<i>suppress</i>	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is 2000 .
<i>max-suppress-time</i>	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is 60 minutes .

	route-map map-name	(OPTIONAL) Enter the keyword <code>route-map</code> then the name of a configured route map. Only <code>match</code> commands in the configured route map are supported.														
Defaults	Disabled.															
Command Modes	- ROUTER BGP - ROUTER BGP-address-family															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	If you enter the <code>bgp dampening</code> command, the default values for <i>half-life</i>, <i>reuse</i>, <i>suppress</i>, and <i>max-suppress-time</i> are applied. The parameters are position-dependent; therefore, if you configure one parameter, configure the parameters in the order they appear in the CLI.															
Related Commands	show ip bgp dampened-paths — views the BGP paths.															

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

Z9500

Syntax	<code>bgp default local-preference value</code> To return to the default value, use the <code>no bgp default local-preference</code> command.	
Parameters	value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value,

the more the route is preferred. The range is from 0 to 4294967295. The default is **100**.

Defaults **100**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information All routers apply the `bgp default local-preference` command setting within the AS. To set the local preference for a specific route, use the `set local-preference` command in ROUTE-MAP mode.

Related Commands [set local-preference](#) — assigns a local preference value for a specific route.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGp peers.

Z9500

Syntax `bgp enforce-first-as`
To turn off the default, use the `no bgp enforce-first-as` command.

Defaults Enabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information

This command is enabled by default, that is for all updates received from EBGp peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is increments. Use the `show ip bgp neighbors` command to view the "failed enforce-first-as check" counter.

If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.

Related Commands

[show ip bgp neighbors](#) — views the information the BGP neighbors exchange.

[show ip protocols](#) — views information on routing protocols.

bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Z9500

Syntax

`bgp fast-external-fallover`

To disable fast external fallover, use the `no bgp fast-external-fallover` command.

Defaults

Enabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The `bgp fast-external-fallover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

Z9500

Syntax	<pre>bgp four-octet-as-support</pre> To disable fast external failover, use the <code>no bgp four-octet-as-support</code> command.
Defaults	Disabled (supports 2-byte format)
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router.

When creating Confederations, all the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

Where the 2-byte format is from 1 to 65535, the 4-byte format is from 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format.

For more information about using the 2 byte or 4-byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

To support graceful restart as a receiver only, enable graceful restart on a BGP neighbor, a BGP node, or designate a local router.

Z9500

Syntax `bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]`

To return to the default, use the `no bgp graceful-restart` command.

Parameters

restart-time seconds	Enter the keyword <code>restart-time</code> then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is 120 seconds .
stale-path-time seconds	Enter the keyword <code>stale-path-time</code> then the maximum number of seconds to wait before restarting a peer's stale paths. The default is 360 seconds .
role receiver-only	Enter the keyword <code>role receiver-only</code> to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

Z9500

Syntax `bgp log-neighbor-changes`
To disable logging, use the `no bgp log-neighbor-changes` command.

Defaults Enabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To view BGP neighbor resets, use the `show logging` command in EXEC mode.

The `bgp log-neighbor-changes` command appears in the `show config` command output.

Related Commands [show logging](#) — views logging settings and system messages logged to the system.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

Z9500

Syntax	<code>bgp non-deterministic-med</code> To return to the default, use the <code>no bgp non-deterministic-med</code> command.
Defaults	Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead the system to choose different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (<code>no bgp non-deterministic-med</code>), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.
--------------------------	--

When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

Z9500

Syntax	<code>bgp recursive-bgp-next-hop</code> To disable next-hop resolution, use the <code>no bgp recursive-bgp-next-hop</code> command.																
Defaults	Enabled																
Command Modes	ROUTER BGP																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.2.1.0</td><td>Introduced.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.	7.2.1.0	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.7.1.0	Introduced on the C-Series.																
7.2.1.0	Introduced.																
Usage Information	This command is a <i>knob</i> to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not. The <code>clear ip bgp</code> command is required for this command to take effect and to keep the BGP database consistent. Execute the <code>clear ip bgp</code> command right after executing this command.																
Related Commands	clear ip bgp — clears the ip bgp.																

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

Z9500

Syntax	<code>bgp regex-eval-optz-disable</code> To re-enable optimization engine, use the <code>no bgp regex-eval-optz-disable</code> command.
Defaults	Enabled
Command Modes	ROUTER BGP (conf-router_bgp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced

Usage Information	BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is common. In a large-scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines. BGP policies, containing regular expressions to match as-path and communities, tend to use much CPU processing time, which in turn affects the BGP routing convergence. Additionally, the <code>show bgp</code> commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.
--------------------------	---

Examples	<pre>Dell(conf-router_bgp)#no bgp regex-eval-optz-disable Dell(conf-router_bgp)#do show ip protocols Routing Protocol is "ospf 22222" Router ID is 2.2.2.2</pre>
-----------------	--

```

Area                    Routing for Networks
51                     10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200

Dell(conf-router_bgp) #

```

Related Commands

[show ip protocols](#) — views information on all routing protocols enabled and active on the E-Series.

bgp router-id

Assign a user-given ID to a BGP router.

Z9500

Syntax

bgp router-id *ip-address*
 To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address

Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

**Usage
Information**

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

Z9500

Syntax

`bgp soft-reconfig-backup`

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults

Off

**Command
Modes**

ROUTER BGP

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

**Usage
Information**

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

**Related
Commands**

[clear ip bgp](#) — activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu neighbor

Enable capture of an IPv4 BGP neighbor packet.

Z9500

Syntax `capture bgp-pdu neighbor ipv4-address direction {both | rx | tx}`

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

Parameters

<i>ipv4-address</i>	Enter the IPv4 address of the target BGP neighbor.
direction {both rx tx}	Enter the keyword <code>direction</code> and a direction — either <code>rx</code> for inbound, <code>tx</code> for outbound, or <code>both</code> .

Defaults Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Related Commands

[capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

[show capture bgp-pdu neighbor](#) — displays BGP packet capture information.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Z9500

Syntax `capture bgp-pdu max-buffer-size 100-102400000`

Parameters `100-10240000` Enter a size for the capture buffer.
`0`

Defaults **40960000 bytes.**

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced

Related Commands [capture bgp-pdu neighbor](#) — enables capture of an IPv4 BGP neighbor packet.

[show capture bgp-pdu neighbor](#) — displays BGP packet capture information for an IPv6 address on the E-Series.

clear ip bgp

Reset BGP sessions on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Z9500

Syntax `clear ip bgp * | as-number | ip-address [flap-statistics | soft [in | out]]`

Parameters `*` Enter an asterisk (`*`) to reset all BGP sessions.

<i>as-number</i>	Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
<i>ip-address</i>	Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
<i>flap-statistics</i>	(OPTIONAL) Enter the keyword <code>flap-statistics</code> to reset the flap statistics on all prefixes from that neighbor.
<i>soft</i>	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
 NOTE: If you enter the <code>clear ip bgp ip-address soft</code> command, both inbound and outbound policies are reset.	
<i>in</i>	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
<i>out</i>	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.
<i><1-4294967295></i>	Enter <code><1-4294967295></code> to clear peers with the AS number.
<i><0.1-65535.65535></i>	Enter <code><0.1-65535.65535></code> to clear peers with the AS number in dot format.
<i>A.B.C.D</i>	Enter the BGP neighbor address in the A.B.C.D format to clear.
<i>X:X:X:X::X</i>	Enter the BGP neighbor address in the X:X:X:X::X format to clear.
<i>dampening</i>	Enter the keyword <code>dampening</code> to clear the flap dampening information.
<i>flap-statistics</i>	Enter the keywords <code>flap-statistics</code> to clear the flap statistics information.
<i>ipv4</i>	Enter the ipv4 address family to clear.
<i>ipv6</i>	Enter the ipv6 address family to clear.
<i>peer-group</i>	Enter the peer-group to clear all members of the peer-group.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the <code>as-number</code> option.

Related Commands

[bgp recursive-bgp-next-hop](#) — disables next-hop resolution through other routes learned by the BGP.

[bgp soft-reconfig-backup](#) — turns on BGP Soft Reconfiguration.

clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

Z9500

Syntax

```
clear ip bgp dampening [ip-address mask]
```

Parameters

ip-address
mask (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.
--------------------------	--

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Z9500

Syntax	<code>clear ip bgp flap-statistics [<i>ip-address mask</i> <i>filter-list as-path-name</i> <i>regex regular-expression</i>]</code>
---------------	--

Parameters	<i>ip-address mask</i>	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
	<i>filter-list as-path-name</i>	(OPTIONAL) Enter the keywords <code>filter-list</code> then the name of a configured AS-PATH list.
	<i>regex regular-expression</i>	(OPTIONAL) Enter the keyword <code>regex</code> then regular expressions. Use one or a combination of the following: • <code>.</code> = (period) any single character (including a white space). • <code>*</code> = (asterisk) the sequences in a pattern (0 or more sequences). • <code>+</code> = (plus) the sequences in a pattern (1 or more sequences). • <code>?</code> = (question mark) sequences in a pattern (either 0 or 1 sequences).  NOTE: Enter an escape sequence (CTRL+v) prior to entering the <code>?</code> regular expression. • <code>[]</code> = (brackets) a range of single-character patterns. • <code>()</code> = (parenthesis) groups a series of pattern elements to a single element. • <code>{ }</code> = (braces) minimum and the maximum match count. • <code>^</code> = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • <code>\$</code> = (dollar sign) the end of the output string.

Command Modes	EXEC Privilege
----------------------	----------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you enter the `clear ip bgp flap-statistics` command without any parameters, all statistics are cleared.

Related Commands

- [show debugging](#) — views the enabled debugging operations.
- [show ip bgp flap-statistics](#) — views the BGP flap statistics.
- [undebug all](#) — disables all debugging operations.

clear ip bgp peer-group

Reset a peer-group's BGP sessions.

Z9500

Syntax `clear ip bgp peer-group peer-group-name`

Parameters

<i>peer-group-name</i>	Enter the peer group name to reset the BGP sessions within that peer group.
------------------------	---

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

Z9500

Syntax	<code>debug ip bgp [<i>ip-address</i> <i>peer-group peer-group-name</i>] [<i>in</i> <i>out</i>]</code>	
	To disable all BGP debugging, use the <code>no debug ip bgp</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group peer-group-name</i>	Enter the keywords <code>peer-group</code> then the name of the peer group to debug.
	<i>in</i>	(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound BGP routes.
	<i>out</i>	(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound BGP routes.
	<i>A.B.C.D</i>	Enter the IP address of peer in the A.B.C.D format.
	<i>X:X:X:X::X</i>	Enter the IPv6 IP address of peer in the X:X:X:X::X format.
	<i>dampening</i>	Enter the keyword <code>dampening</code> to view BGP dampening.
	<i>events</i>	Enter the keyword <code>events</code> to view BGP protocol events.
	<i>ipv4</i>	Enter the ipv4 IP address to view the IPV4 route information.
	<i>ipv6</i>	Enter the ipv6 IP address to view the IPV6 route information.
	<i>keepalives</i>	Enter the keyword <code>keepalives</code> to view BGP keepalives.
	<i>notifications</i>	Enter the keyword <code>notifications</code> to view BGP notifications.
	<i>soft-reconfiguration</i>	Enter the keywords <code>soft-reconfiguration</code> to view only information on inbound BGP soft reconfiguration.
	<i>updates</i>	Enter the keyword <code>updates</code> to view BGP updates.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter the `debug ip bgp in` command and then enter the `debug ip bgp out` command, you do not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

[debug ip bgp events](#) — views information about BGP events.

[debug ip bgp keepalives](#) — views information about BGP keepalives.

[debug ip bgp notifications](#) — views information about BGP notifications.

[debug ip bgp updates](#) — views information about BGP updates.

[show debugging](#) — views enabled debugging operations.

debug ip bgp dampening

View information on routes being dampened.

Z9500

Syntax

```
debug ip bgp ipv4 multicast dampening
```

To disable debugging, use the `no debug ip bgp ipv4 multicast dampening` command.

Parameters

dampening

Enter the keyword `dampening` to clear route flap dampening information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced IPv6 MGBP support for the E-Series.

debug ip bgp events

Display information on local BGP state changes and other BGP events.

Z9500

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name] events
[in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] events` command.

Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group peer-group-name</i>	(OPTIONAL) Enter the keyword <code>peer-group</code> then the name of the peer group.
	<i>in</i>	(OPTIONAL) Enter the keyword <code>in</code> to view only events on inbound BGP messages.
	<i>out</i>	(OPTIONAL) Enter the keyword <code>out</code> to view only events on outbound BGP messages.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp keepalives

Display information about BGP keepalive messages.

Z9500

Syntax `debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]`
 To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group peer-group-name</i>	(OPTIONAL) Enter the keyword <code>peer-group</code> then the name of the peer group.
<i>in</i>	(OPTIONAL) Enter the keyword <code>in</code> to view only inbound keepalive messages.
<i>out</i>	(OPTIONAL) Enter the keyword <code>out</code> to view only outbound keepalive messages.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

Z9500

Syntax `debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]`
To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group <i>peer-group-name</i>	(OPTIONAL) Enter the keyword <code>peer-group</code> then the name of the peer group.
<i>in</i>	(OPTIONAL) Enter the keyword <code>in</code> to view BGP notifications received from neighbors.
<i>out</i>	(OPTIONAL) Enter the keyword <code>out</code> to view BGP notifications sent to neighbors

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp soft-reconfiguration

Enable soft-reconfiguration debug.

Z9500

Syntax `debug ip bgp {ip-address | peer-group-name} soft-reconfiguration`
To disable, use the `no debug ip bgp {ip-address | peer-group-name} soft-reconfiguration` command.

Parameters

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group..

Defaults Disabled

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

**Usage
Information**

This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug turns on for all neighbors.

debug ip bgp updates

Allows you to view information about BGP updates.

Z9500

Syntax

```
debug ip bgp updates [in | out | prefix-list prefix-list-name]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] updates [in | out]` command.

Parameters

in	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.
prefix-list prefix-list- name	(OPTIONAL) Enter the keyword <code>prefix-list</code> then the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group- name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

**Command
Modes**

EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	To remove all configured debug commands for BGP, enter the <code>no debug ip bgp</code> command.
-------------------	--

default-metric

Allows you to change the metric of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

Z9500

Syntax	<code>default-metric number</code> To return to the default setting, use the <code>no default-metric</code> command.
--------	---

Parameters	<i>number</i>	Enter a number as the metric to be assigned to routes from other protocols. The range is from 1 to 4294967295.
------------	---------------	--

Defaults	0
----------	---

Command Modes	ROUTER BGP
---------------	------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	The <code>default-metric</code> command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.
-------------------	---

Related Commands	bgp always-compare-med — enables comparison of all BGP MED attributes. redistribute — redistributes routes from other routing protocols into BGP.
------------------	--

description

Enter a description of the BGP routing protocol

Z9500

Syntax	description { <i>description</i> }															
	To remove the description, use the no description { <i>description</i> } command.															
Parameters	<i>description</i>	Enter a description to identify the BGP protocol (80 characters maximum).														
Defaults	none															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Related Commands	router bgp — enters ROUTER mode on the switch.															

distance bgp

Define an administrative distance for routes.

Z9500

Syntax	<code>distance bgp external-distance internal-distance local-distance</code> To return to default values, use the <code>no distance bgp</code> command.	
Parameters	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is 20 .

<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is 200 .
<i>local-distance</i>	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is 200 .

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes

ROUTER BGP (conf-router_bgp_af)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced IPv6 MGBP on the E-Series.

Usage Information



CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

max-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Z9500

Syntax

`max-paths {ebgp | ibgp} number`

To return to the default values, enter the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.
-------------	--

	ibgp	Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes.																
	<i>number</i>	Enter a number as the maximum number of parallel paths.																
Defaults	none																	
Command Modes	ROUTER BGP																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.8.0</td><td>Support from 2 to 64 paths on the S4810. Command syntax changed to <code>max-path</code> (was maximum-paths).</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Support from 2 to 64 paths on the S4810. Command syntax changed to <code>max-path</code> (was maximum-paths).	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.8.0	Support from 2 to 64 paths on the S4810. Command syntax changed to <code>max-path</code> (was maximum-paths).																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.7.1.0	Introduced on the C-Series.																	
Usage Information	If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.																	

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

Z9500

Syntax	<pre>neighbor [<i>ip-address</i> <i>peer-group-name</i>] activate</pre> To disable, use the <code>no neighbor [<i>ip-address</i> <i>peer-group-name</i>] activate</code> command.	
Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
	activate	Enter the keyword <code>activate</code> to enable the neighbor/peer group in the new AFI/SAFI.

Defaults	Disabled														
Command Modes	CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. When you use <code>activate</code> in the new context, the neighbor/peer group enables for AFI/SAFI.														

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

Z9500

Syntax	<code>neighbor [ip-address peer-group-name] add-path [send receive both] path-count</code>	
Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
	<i>send</i>	Enter the keyword <code>send</code> to indicate that the system sends multiple paths to peers.
	<i>receive</i>	Enter the keyword <code>receive</code> to indicate that the system accepts multiple paths from peers.
	<i>both</i>	Enter the keyword <code>both</code> to indicate that the system sends and accepts multiple paths from peers.
	<i>path-count</i>	Enter the number paths supported. The range is from 2 to 64.
Defaults	none	

Command Modes	CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.8.0	Introduced on the S4810.										
Related Commands	bgp add-path — allows the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones.										

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} advertisement-interval seconds</pre> To return to the default value, use the <code>no neighbor {ip-address peer-group-name} advertisement-interval</code> command.	
Parameters	<i>ip-address</i> <i>peer-group-name</i> <i>seconds</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format. Enter the name of the peer group to set the advertisement interval for all routers in the peer group. Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is 5 seconds for internal BGP peers and 30 seconds for external BGP peers.
Defaults	- seconds = 5 seconds (internal peers) - seconds = 30 seconds (external peers)	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor advertisement-start

To send BGP routing updates, set the minimum interval before starting.

Z9500

Syntax	<code>neighbor {ip-address} advertisement-start seconds</code> To return to the default value, use the <code>no neighbor {ip-address} advertisement-start</code> command.	
Parameters	<i>ip-address</i> (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format. <i>seconds</i> Enter a number as the time interval, in seconds, before BGP route updates are sent. The range is from 0 to 3600 seconds.	
Defaults	none	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} allowas-in number</pre> To return to the default value, use the <code>no neighbor {ip-address peer-group-name} allowas-in</code> command.	
Parameters	ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	number	Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Related Commands	bgp four-octet-as-support — enables 4-byte support for the BGP process.
------------------	---

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} default-originate [route-map map-name]</pre>
--------	---

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the default route of all routers in that peer group.
<i>route-map map-name</i>	(OPTIONAL) Enter the keyword <code>route-map</code> then the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

Z9500

Syntax

`neighbor {ip-address | peer-group-name} description text`
To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

Parameters

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
--------------------------	--

	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>text</i>	Enter a continuous text string up to 80 characters.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor distribute-list

Distribute BGP information via an established prefix list.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}
```

To delete a neighbor distribution list, use the `no neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
	<i>prefix-list-name</i>	Enter the name of an established prefix list.
		If the prefix list is not configured, the default is permit (to allow all routes).
	<i>in</i>	Enter the keyword <code>in</code> to distribute only inbound traffic.

	out	Enter the keyword <code>out</code> to distribute only outbound traffic.														
Defaults	Not configured.															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	Other BGP filtering commands include: <code>neighbor filter-list</code> , <code>ip as-path access-list</code> , and <code>neighbor route-map</code> .															
Related Commands	ip as-path access-list — configures IP AS-Path ACL. neighbor filter-list — assigns a AS-PATH list to a neighbor or peer group. neighbor route-map — assigns a route map to a neighbor or peer group.															

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} ebgp-multihop [ttl]</pre> To disallow and disconnect connections, use the <code>no neighbor {ip-address peer-group-name} ebgp-multihop</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>ttl</i>	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is from 1 to 255. The default is 255 .

Defaults	Disabled.														
Command Modes	ROUTER BGP														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	To prevent loops, the <code>neighbor ebgp-multihop</code> command does not install the default routes of the multihop peer. Networks not directly connected are not considered valid for best-path selection.														

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Z9500

Syntax	<code>neighbor {<i>ipv4-address</i> <i>peer-group-name</i>} fall-over</code> To disable, use the <code>no neighbor {<i>ipv4-address</i> <i>peer-group-name</i>} fall-over</code> command.	
Parameters	<i>ipv4-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group.
Defaults	Disabled.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information

When you enable failover, BGP keeps track of IP or IPv6 ability to reach the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for the peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

[show ip bgp neighbors](#) — displays information on the BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}
```

To delete a BGP filter, use the `no neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}` command.

Parameters

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
<i>as-path-name</i>	Enter the name of an established AS-PATH access list (up to 140 characters). If the AS-PATH access list is not configured, the default is permit (allow routes).
<i>in</i>	Enter the keyword <code>in</code> to filter inbound BGP routes.
<i>out</i>	Enter the keyword <code>out</code> to filter outbound BGP routes.

Defaults

Not configured.

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series. Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, ACL names were up to 16 characters long.
7.7.1.0	Introduced on the C-Series.

Usage Information

To enter AS-PATH ACL mode and configure the AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute, use the `ip as-path access-list` command in CONFIGURATION mode.

Related Commands

[ip as-path access-list](#) — enter AS-PATH ACL mode and configure the AS-PATH filters.

neighbor graceful-restart

Enable graceful restart on a BGP neighbor.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} graceful-restart  
[restart-time seconds] [stale-path-time seconds] [role  
receiver-only]
```

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
<i>restart-time seconds</i>	Enter the keyword <code>restart-time</code> then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is 120 seconds .
<i>stale-path-time seconds</i>	Enter the keyword <code>stale-path-time</code> then the maximum number of seconds to wait before restarting a peer's stale paths. The default is 360 seconds .

	role receiver-only	Enter the keyword <code>role receiver-only</code> to designate the local router to support graceful restart as a receiver only.														
Defaults	as above															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	This feature advertises to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.															

neighbor local-as

To accept external routes from neighbors with a local AS number in the AS number path, configure Internal BGP (IBGP) routers.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} local-as as-number [no-prepend]</pre> To return to the default value, use the <code>no neighbor {ip-address peer-group-name} local-as</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>as-number</i>	Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte) or from 0.1 to 65535.65535 (dotted format).

	no prepend	Specifies that local AS values do not prepend to announcements from the neighbor.														
Defaults	Not configured.															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Related Commands	bgp four-octet-as-support — enables 4-byte support for the BGP process.															

neighbor maximum-prefix

Control the number of network prefixes received.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} maximum-prefix maximum [threshold] [warning-only]</pre> To return to the default values, use the <code>no neighbor {ip-address peer-group-name} maximum-prefix maximum</code> command.	
Parameters	ip-address	Enter the IP address of the neighbor in dotted decimal format.
	peer-group-name	Enter the name of the peer group.
	maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
	threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the E-Series software sends a message. The range is from 1 to 100 percent. The default is 75 .

	warning-only	(OPTIONAL) Enter the keyword <code>warning-only</code> to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.														
Defaults	threshold = 75															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	If you configure the <code>neighbor maximum-prefix</code> command and the neighbor receives more prefixes than the <code>neighbor maximum-prefix</code> command configuration allows, the neighbor goes down and the <code>show ip bgp summary</code> command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the <code>clear ip bgp</code> command for the neighbor or the peer group to which the neighbor belongs or you enter the <code>neighbor shutdown</code> and <code>neighbor no shutdown</code> commands.															
Related Commands	show ip bgp summary — displays the current BGP configuration.															

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Z9500

Syntax	<pre>neighbor {ipv6-address peer-group-name} next-hop-self</pre> To return to the default setting, use the <code>no neighbor {ipv6-address peer-group-name} next-hop-self</code> command.	
Parameters	ipv6-address	Enter the IPv6 address in the x:x:x:x::x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.

	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
Defaults	Disabled.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you configure the <code>set ipv6 next-hop</code> command in ROUTE-MAP mode, its configuration takes precedence over the <code>neighbor next-hop-self</code> command.	

neighbor password

Enable message digest 5 (MD5) authentication on the TCP connection between two neighbors.

Z9500

Syntax	<code>neighbor {ip-address peer-group-name} password [encryption-type] password</code> To delete a password, use the <code>no neighbor {ip-address peer-group-name} password</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.
	<i>peer-group-name</i>	Enter the name of a configured peer group.
	<i>encryption-type</i>	(OPTIONAL) Enter 7 as the encryption type for the password entered. 7 means that the password is encrypted and hidden.
	<i>password</i>	Enter a text string up to 80 characters long. The first character of the password must be a letter. You cannot use spaces in the password.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from
[peer's IP address] : 11502 to [local router's IP address] :179
```

neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

Z9500

Syntax

```
neighbor ip-address peer-group peer-group-name
```

To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

Parameters

<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.
--------------------------	--

	<i>peer-group-name</i> Enter the name of a configured peer group.														
Defaults	Not configured.														
Command Modes	ROUTER BGP														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	You can assign up to 256 peers to one peer group. When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer: • neighbor advertisement-interval • neighbor distribute-list • neighbor filter-list • neighbor route-map • neighbor route-reflector-client • neighbor send-community A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates. A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).														
Related Commands	clear ip bgp — resets BGP sessions. neighbor peer-group (creating group) — creates a peer group. show ip bgp peer-group — views BGP peers.														

[show ip bgp neighbors](#) — views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

Z9500

Syntax `neighbor peer-group-name peer-group`
To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters

<i>peer-group-name</i>	Enter a text string up to 16 characters long as the name of the peer group.
-------------------------------	---

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information When you create a peer group, it is disabled (Shut mode).

Related Commands

[neighbor peer-group \(assigning peers\)](#) — assigns routers to a peer group.

[neighbor remote-as](#) — assigns a indirectly connected AS to a neighbor or peer group.

[neighbor shutdown](#) — disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

Z9500

Syntax	neighbor <i>peer-group-name</i> peer-group passive [<i>sessions</i>] To delete a passive peer-group, use the no neighbor <i>peer-group-name</i> peer-group passive command.																	
Parameters	<i>peer-group-name</i>	Enter a text string up to 16 characters long as the name of the peer group.																
Defaults	Not configured.																	
Command Modes	ROUTER BGP																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.8.0</td><td>Introduced the <code>limit</code> keyword on the S4810.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Introduced the <code>limit</code> keyword on the S4810.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.8.0	Introduced the <code>limit</code> keyword on the S4810.																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.7.1.0	Introduced on the C-Series.																	
Usage Information	After you configure a peer group as passive, assign it a subnet using the neighbor <code>soft-reconfiguration inbound</code> command. For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.																	
Related Commands	neighbor soft-reconfiguration inbound — assigns a subnet to a dynamically configured BGP neighbor. neighbor remote-as — assigns an indirectly connected AS to a neighbor or peer group.																	

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Z9500

Syntax	<code>neighbor {ip-address peer-group-name} remote-as number</code> To delete a remote AS entry, use the <code>no neighbor {ip-address peer-group-name} remote-as number</code> command.															
Parameters	ip-address	Enter the IP address of the neighbor to enter the remote AS in its routing table.														
	peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.														
	number	Enter a number of the AS. The range is from 0 to 65535 (2 byte) or from 1 to 4294967295 (4 byte).														
Defaults	Not configured.															
Command Modes	ROUTER BGP															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series. Added 4-byte support.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series. Added 4-byte support.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series. Added 4-byte support.															
Usage Information	To accept 4-byte formats before entering a 4 byte AS Number, configure your system. If the <code>number</code> parameter is the same as the AS number used in the <code>router bgp</code> command, the remote AS entry in the neighbor is considered an internal BGP peer entry. This command creates a peer and the newly created peer is disabled (Shutdown).															
Related Commands	router bgp — enters ROUTER BGP mode and configures routes in an AS.															

[bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Z9500

Syntax	neighbor {ip-address peer-group-name} remove-private-as To return to the default, use the no neighbor {ip-address peer-group-name} remove-private-as command.	
Parameters	ip-address	Enter the IP address of the neighbor to remove the private AS numbers.
	peer-group-name	Enter the name of the peer group to remove the private AS numbers.
Defaults	Disabled (that is, private AS number are not removed).	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Introduced on the S-Series.
	7.7.1.0	Introduced on the C-Series. Added 4-byte support.
Usage Information	Applies to EBGp neighbors only. Configure your system to accept 4-byte formats before entering a 4 byte AS Number. If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGp neighbor, the private AS numbers are not removed. If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.	

Private AS numbers are from 64512 to 65535 (2 byte).

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Z9500

Syntax `neighbor {ip-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ip-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
in	Enter the keyword <code>in</code> to filter inbound routes.
out	Enter the keyword <code>out</code> to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

**Usage
Information**

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

Z9500

Syntax

`neighbor {ip-address | peer-group-name} route-reflector-client`

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

ip-address

Enter the IP address of the neighbor in dotted decimal format.

peer-group-name

Enter the name of the peer group.

All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

**Command
Modes**

ROUTER BGP

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need to be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

Related Commands

[bgp client-to-client reflection](#) — enables route reflection between the route reflector and the clients.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} send-community
```

To disable sending a COMMUNITY attribute, use the `no neighbor {ip-address | peer-group-name} send-community` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.
extended	Optional. Enter the keyword <code>extended</code> to send extended community attribute.
standard	Optional. Enter the keyword <code>standard</code> to send standard community attribute.

Defaults

Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To configure a COMMUNITY attribute, use the `set community` command in ROUTE-MAP mode.

Before using this command, you must execute the `clear ip bgp` command.

neighbor shutdown

Disable a BGP neighbor or peer group.

Z9500

Syntax

`neighbor {ip-address | peer-group-name} shutdown`

To enable a disabled neighbor or peer group, use the `neighbor {ip-address | peer-group-name} no shutdown` command.

Parameters

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	Peers that are enabled within a peer group are disabled when their peer group is disabled. The <code>neighbor shutdown</code> command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shut down, use the <code>show ip bgp summary</code> command to confirm its status.
Related Commands	show ip bgp summary — displays the current BGP configuration. show ip bgp neighbors — displays the current BGP neighbors.

neighbor soft-reconfiguration inbound

Enable soft-reconfiguration for BGP.

Z9500

Syntax	<code>neighbor {ip-address peer-group-name} soft-reconfiguration inbound</code> To disable, use the <code>no neighbor {ip-address peer-group-name} soft-reconfiguration inbound</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to disable or enable all routers within the peer group.
Defaults	Disabled	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.4.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	7.4.1.0	Introduced.
Version	Description				
7.4.1.0	Introduced.				
Usage Information	This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates the neighbor receives but does not reset the peer-session.  CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.  NOTE: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only. Related Commands show ip bgp neighbors — displays routes received by a neighbor.				

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

Z9500

Syntax	<pre>neighbor peer-group-name subnet subnet-number mask</pre> To remove passive peering, use the <code>no neighbor peer-group-name subnet subnet-number mask</code> command.				
Parameters	<table> <tr> <td>subnet-number</td><td> Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0.0.0.0/0. </td></tr> <tr> <td>mask</td><td> Enter a prefix mask in / prefix-length format (/x). </td></tr> </table>	subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0.0.0.0/0.	mask	Enter a prefix mask in / prefix-length format (/x).
subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0.0.0.0/0.				
mask	Enter a prefix mask in / prefix-length format (/x).				
Defaults	Not configured.				
Command Modes	ROUTER BGP				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.				

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Z9500

Syntax

```
neighbor {ip-address | peer-group-name} timers keepalive
holdtime
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} timers` command.

Parameters	<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the timers for all routers within the peer group.
	<i>keepalive</i>	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is 60 seconds .
	<i>holdtime</i>	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is 180 seconds .

- Defaults**
- keepalive = **60 seconds**
 - holdtime = **180 seconds**

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	7.7.1.0	Introduced on the C-Series.
Version	Description				
7.7.1.0	Introduced on the C-Series.				
Usage Information	Timer values configured with the <code>neighbor timers</code> command override the timer values configured with any other command. When two neighbors, configured with different <code>keepalive</code> and <code>holdtime</code> values, negotiate for new values, the resulting values are as follows: - the lower of the <code>holdtime</code> value is the new <code>holdtime</code> value, and - whichever is the lower value; one-third of the new <code>holdtime</code> value, or the configured <code>keepalive</code> value, is the new <code>keepalive</code> value.				

neighbor update-source

Enable the system to use Loopback interfaces for TCP connections for BGP sessions.

Z9500

Syntax	<pre>neighbor {ip-address peer-group-name} update-source interface</pre> To use the closest interface, use the <code>no neighbor {ip-address peer-group-name} update-source interface</code> command.	
Parameters	<i>ip-address</i> Enter the IP address of the peer router in dotted decimal format. <i>peer-group-name</i> Enter the name of the peer group to disable all routers within the peer group. <i>interface</i> Enter the keyword <code>loopback</code> then a number of the Loopback interface. The range is from 0 to 16383.	
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

	Version	Description
	7.8.1.0	Introduced on the S-Series.
	7.7.1.0	Introduced on the C-Series.
Usage Information	Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The <code>neighbor update-source</code> command is not necessary for directly connected internal BGP sessions.	

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Z9500

Syntax	<code>neighbor {ip-address peer-group-name} weight weight</code> To remove a weight value, use the <code>no neighbor {ip-address peer-group-name} weight</code> command.	
Parameters	ip-address	Enter the IP address of the peer router in dotted decimal format.
	peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
	weight	Enter a number as the weight. The range is from 0 to 65535. The default is 0 .
Defaults	0	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

In the best path selection process, the path with the highest weight value is preferred.



NOTE: In the best-path selection process, the path with the highest weight value is preferred.

If you configure the `set weight` command in a route map applied to this neighbor, the weight set in that command overrides the weight set in the `neighbor weight` command.

Related Commands

[set weight](#) — assigns a weight to all paths meeting the route map criteria.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Z9500

Syntax

```
network ip-address mask [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ip-address

Enter an IP address in dotted decimal format of the network.

mask

Enter the mask of the IP address in the slash prefix length format (for example, /24).

The mask appears in command outputs in dotted decimal format (A.B.C.D).

route-map map-name

(OPTIONAL) Enter the keyword `route-map` then the name of an established route map.

Only the following ROUTE-MAP mode commands are supported:

- [match ip address](#)
- [set community](#)
- [set local-preference](#)
- [set metric](#)
- [set next-hop](#)
- [set origin](#)
- [set weight](#)

If the route map is not configured, the default is **deny** (to drop all routes).

Defaults	Not configured.														
Command Modes	ROUTER BGP														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	The system resolves the network address the <code>network</code> command configures with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.														
Related Commands	redistribute — redistributes routes into BGP.														

network backdoor

Specify this IGP route as the preferred route.

Z9500

Syntax	<pre>network ip-address mask backdoor</pre> To remove a network, use the <code>no network ip-address mask backdoor</code> command.	
Parameters	<i>ip-address</i> Enter an IP address in dotted decimal format of the network. <i>mask</i> Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).	
Defaults	Not configured.	
Command Modes	ROUTER BGP	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Although the system does not generate a route due to the backdoor config, there is an option for injecting/sourcing a local route in the presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

Z9500

Syntax

```
redistribute {connected | static} [route-map map-name]
```

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

connected	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
static	Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map <i>map-name</i>	(OPTIONAL) Enter the keyword <code>route-map</code> then the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric

- [set next-hop](#)
- [set origin](#)
- [set weight](#)

If the route map is not configured, the default is **deny** (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as internal .
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information You can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and applied outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.

Related Commands [neighbor default-originate](#) — injects the default route.

redistribute ospf

Redistribute OSPF routes into BGP.

Z9500

Syntax `redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]`
To stop redistribution of OSPF routes, use the `no redistribute ospf process-id` command.

Parameters	process-id	Enter the number of the OSPF process. The range is from 1 to 65535.
	match external {1 2}	(OPTIONAL) Enter the keywords <code>match external</code> to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
	match internal	(OPTIONAL) Enter the keywords <code>match internal</code> to redistribute OSPF internal routes only.
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as internal .
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information You can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and

apply outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

When you enter the `redistribute isis process-id` command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. RFC does not support this feature.

router bgp

To configure and enable BGP, enter ROUTER BGP mode.

Z9500

Syntax

```
router bgp as-number
```

To disable BGP, use the `no router bgp as-number` command.

Parameters

as-number

Enter the AS number. The range is from 1 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

At least one interface must be in Layer 3 mode for the `router bgp` command to be accepted. If no interfaces are enabled for Layer 3, an error message appears:

```
% Error: No router id configured
```

Example

```
Dell(conf)#router bgp 3
Dell(conf-router_bgp)#
```


show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

Z9500

Syntax	<code>show capture bgp-pdu neighbor ipv4-address</code>	
Parameters	<i>ipv4-address</i>	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Example

```
Dell(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using
680 bytes
  PDU[1] : len 101, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00650100 00000013
00000000
00000000 419ef06c 00000000
  00000000 00000000 00000000 00000000 0181a1e4 0181a25c
41af92c0
00000000 00000000 00000000
  00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
[. . .]
```

```
Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using
562 bytes
  PDU[1] : len 41, captured 00:34:52 ago
    ffffffff ffffffff ffffffff ffffffff 00290104 000100b4
```

```

14141401
0c020a01 04000100 01020080
00000000
PDU[2] : len 19, captured 00:34:51 ago
ffffffff ffffffff ffffffff ffffffff 00130400
PDU[3] : len 19, captured 00:34:50 ago
ffffffff ffffffff ffffffff ffffffff 00130400
[. . .]
Dell#

```

Related Commands [capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

Z9500

Syntax	show config
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Example

```

Dell(conf-router_bgp)#show config
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
Dell(conf-router_bgp)#

```

Related Commands [capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

show ip bgp

View the current BGP IPv4 routing table for the system.

Z9500

Syntax	<code>show ip bgp [ipv4 unicast] [network [network-mask] [longer-prefixes]]</code>																	
Parameters	ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.																
	network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.																
	network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.																
	longer-prefixes	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.																
Command Modes	- EXEC - EXEC Privilege																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.8.0</td><td>Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.8.0	Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.7.1.0	Introduced on the C-Series.																	
Usage Information	When you enable the <code>bgp non-deterministic-med</code> command, the <code>show ip bgp</code> command output for a BGP route does not list the INACTIVE reason. The following describes the <code>show ip bgp</code> command shown in the following example.																	

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network      Next Hop    Metric LocPrf Weight Path
*>  0.0.0.0/0      63.114.8.33          0 18508 i
*   3.0.0.0/8      63.114.8.33          0 18508 209
701 80 i
*>                63.114.8.33          0 18508 701 80
i
*>  3.3.0.0/16      0.0.0.0             22      32768 ?
                        63.114.8.35          0 18508 ?
*>  4.0.0.0/8      63.114.8.33          0 18508 701 1 i
*>  4.2.49.12/30    63.114.8.33          0 18508 209 i
*   4.17.250.0/24   63.114.8.33          0 18508 209
1239 13716 i
*>  63.114.8.33          0 18508 701
1239 13716 i
*   4.21.132.0/23   63.114.8.33          0 18508 209
6461 16422 i
*>                63.114.8.33          0 18508 701
6461 16422 i
*>  4.24.118.16/30   63.114.8.33          0 18508 209 i
*>  4.24.145.0/30    63.114.8.33          0 18508 209 i
*>  4.24.187.12/30   63.114.8.33          0 18508 209 i
*>  4.24.202.0/30    63.114.8.33          0 18508 209 i
*>  4.25.88.0/30     63.114.8.33          0 18508 209
3561 3908 i
*>  5.0.0.0/9      63.114.8.33          0      0 18508 ?
*>  5.0.0.0/10      63.114.8.33          0      0 18508 ?
*>  5.0.0.0/11      63.114.8.33          0      0 18508 ?
--More--
```

Related Commands

[show ip bgp community](#) — views the BGP communities.

[neighbor maximum-prefix](#) — controls the number of network prefixes received.

show ip bgp cluster-list

View BGP neighbors in a specific cluster.

Z9500

Syntax	show ip bgp [<i>ipv4 unicast</i>] cluster-list [<i>cluster-id</i>]															
Parameters	<i>ipv4 unicast</i>	(OPTIONAL) Enter the keywords <i>ipv4 unicast</i> to view information only related to ipv4 unicast routes.														
	<i>cluster-id</i>	(OPTIONAL) Enter the cluster id in dotted decimal format. The range is 1 — 4294967295.														
Command Modes	- EXEC - EXEC Privilege															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	The following describes the <code>show ip bgp cluster-list</code> command shown in the following example. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Network</td><td>Displays the destination network prefix of each BGP route.</td></tr><tr><td>Next Hop</td><td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td></tr><tr><td>Metric</td><td>Displays the BGP route's metric, if assigned.</td></tr><tr><td>LocPrf</td><td>Displays the BGP LOCAL_PREF attribute for the route.</td></tr><tr><td>Weight</td><td>Displays the route's weight.</td></tr></table>		Field	Description	Network	Displays the destination network prefix of each BGP route.	Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.	Metric	Displays the BGP route's metric, if assigned.	LocPrf	Displays the BGP LOCAL_PREF attribute for the route.	Weight	Displays the route's weight.		
Field	Description															
Network	Displays the destination network prefix of each BGP route.															
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.															
Metric	Displays the BGP route's metric, if assigned.															
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.															
Weight	Displays the route's weight.															

Field	Description
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp cluster-list
BGP table version is 64444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n
- network
Origin codes: i - IGP, e - EGP, ? - incomplete
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
* I	10.10.10.1/32	192.68.16.1	0	100	0	i
* I		192.68.16.1	0	100	0	i
*>I		192.68.16.1	0	100	0	i
* I		192.68.16.1	0	100	0	i
* I		192.68.16.1	0	100	0	i
* I		192.68.16.1	0	100	0	i
* I	10.19.75.5/32	192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
*>I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
* I	10.30.1.0/24	192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
*>I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?
* I		192.68.16.1	0	100	0	?

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

Z9500

Syntax

```
show ip bgp [ipv4 unicast] community [community-number] [local-as] [no-export] [no-advertise]
```

Parameters

ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords <code>local-AS</code> to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED.

	All routes with the NO_EXPORT_SUBCONFED (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.														
no-advertise	Enter the keywords <code>no-advertise</code> to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.														
no-export	Enter the keywords <code>no-export</code> to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.														
Command Modes	- EXEC - EXEC Privilege														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.8.1.0	Introduced on the S-Series.														
7.7.1.0	Introduced on the C-Series.														
Usage Information	To view the total number of COMMUNITY attributes found, use the <code>show ip bgp summary</code> command. The text line above the route table states the number of COMMUNITY attributes found. The <code>show ip bgp community</code> command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the <code>show ip bgp</code> command output. The following describes the <code>show ip bgp community</code> command shown in the following example.														

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```

Dell>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop    Metric LocPrf Weight Path
* i 3.0.0.0/8     205.171.0.16      100    0 209 701 80 i
*>i 4.2.49.12/30   205.171.0.16      100    0 209 i
* i 4.21.132.0/23 205.171.0.16      100    0 209 6461
16422 i
*>i 4.24.118.16/3  205.171.0.16      100    0 209 i
*>i 4.24.145.0/30  205.171.0.16      100    0 209 i
*>i 4.24.187.12/30 205.171.0.16      100    0 209 i
*>i 4.24.202.0/30  205.171.0.16      100    0 209 i
*>i 4.25.88.0/30   205.171.0.16      100    0 209 3561 3908
i
*>i 6.1.0.0/16     205.171.0.16      100    0 209 7170 1455
i
*>i 6.2.0.0/22     205.171.0.16      100    0 209 7170 1455
i
*>i 6.3.0.0/18     205.171.0.16      100    0 209 7170 1455
i
*>i 6.4.0.0/16     205.171.0.16      100    0 209 7170 1455
i
*>i 6.5.0.0/19     205.171.0.16      100    0 209 7170 1455
i
*>i 6.8.0.0/20     205.171.0.16      100    0 209 7170 1455
i
*>i 6.9.0.0/20     205.171.0.16      100    0 209 7170 1455
i
*>i 6.10.0.0/15    205.171.0.16      100    0 209 7170 1455
i
*>i 6.14.0.0/15    205.171.0.16      100    0 209 7170 1455
i
*>i 6.133.0.0/21   205.171.0.16      100    0 209 7170 1455
i
*>i 6.151.0.0/1    205.171.0.16      100    0 209 7170 1455
i
--More--

```


show ip bgp community-list

View routes that a specific community list affects.

Z9500

Syntax	show ip bgp [ipv4 unicast] community-list community-list-name [exact-match]															
Parameters	ipv4 unicast	(OPTIONAL) Enter the keywords ipv4 unicast to view information only related to ipv4 unicast routes.														
	community-list-name	Enter the name of a configured IP community list (maximum 140 characters).														
	exact-match	Enter the keyword for an exact match of the communities.														
Command Modes	- EXEC - EXEC Privilege															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	The show ip bgp community-list command without any parameters lists BGP routes matching the Community List and the output is the same as for the show ip bgp command output. The following describes the show ip bgp community-list pass command shown in the following example. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Network</td><td>Displays the destination network prefix of each BGP route.</td></tr><tr><td>Next Hop</td><td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td></tr></table>		Field	Description	Network	Displays the destination network prefix of each BGP route.	Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.								
Field	Description															
Network	Displays the destination network prefix of each BGP route.															
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.															

Field	Description
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network      Next Hop      Metric      LocPrf      Weight Path
Dell#
```

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Z9500

Syntax	<code>show ip bgp [ipv4 unicast] dampened-paths</code>
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information	The following describes the <code>show ip bgp damp</code> command shown in the following example.
--------------------------	---

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      From      Reuse      Path
Dell>
```

show ip bgp detail

Display BGP internal information for the IPv4 Unicast address family.

Z9500

Syntax	<code>show ip bgp [ipv4 unicast] detail</code>
Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Example

```
Dell#show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 :
NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 :
NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP
0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP
0x41a190a0 :
NdRRClstTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 :
NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP :
NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 :
NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 :
NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP
0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRtDamp 0 : AlwaysCmpMed 0 : LocrHld
10 : LocrRem 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops
0 : Opens 0
Closes 0 : Fails 0 : FataIs 0 : ConnExps 0 : HldExps 0 :
KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 :
TxNotifs 0
BadEvs 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP
0x41a1b6d4 : RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP
0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP
0x41a1b7b8 : LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl
0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 :
CleanRibTmrP 0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP
0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : Enforce1stAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 :
NonDet 0 : DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 :
IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 :
MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
```

```

Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP
0x41a19d28 : NdRTMAFTblVer 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen
0 : NdAFWPtRP 0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd
1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP
0x41a0d600 : AfAggCtxAddr
1101111028 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 :
AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrLen 255 : AfEorSet
0x41a19f98 : NumDfrdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist
200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr
1101112392 :
AfNetCtxAddrLen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrLen 255 : AfNetBKDrRttP
0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling
0 : AfDampRmapP

```

show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

Z9500

Syntax	show ip bgp [<i>ipv4 unicast</i>] extcommunity-list [<i>list name</i>]	
Parameters	<i>ipv4 unicast</i>	(OPTIONAL) Enter the keywords <i>ipv4 unicast</i> to view information only related to <i>ipv4 unicast</i> routes.
	<i>list name</i>	Enter the extended community list name you wish to view. The range is 140 characters.
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>	

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp filter-list

View the routes that match the filter lists.

Z9500

Syntax

```
show ip bgp [ipv4 unicast] filter-list as-path-name
```

Parameters

<i>ipv4 unicast</i>	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
<i>as-path-name</i>	Enter an AS-PATH access list name. The range is 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp filter-list hello` command shown in the following example.

Field	Description
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: - i = internal route entry - a = aggregate route entry - c = external confederation route entry - n = network route entry - r = redistributed route entry
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n -
network
Origin codes: i - IGP, e - EGP, ? - incomplete
```

	Network	Next Hop	Metric	LocPrf	Weight
Path					
* I	6.1.5.0/24	192.100.11.2	20000	9999	0 ?
* I		192.100.8.2	20000	9999	0 ?
* I		192.100.9.2	20000	9999	0 ?
* I		192.100.10.2	20000	9999	0 ?
*>I		6.1.5.1	20000	9999	0 ?
* I		6.1.6.1	20000	9999	0 ?
* I		6.1.20.1	20000	9999	0 ?
* I		6.1.6.0/24 192.100.11.2	20000	9999	0 ?
* I		192.100.8.2	20000	9999	0 ?
* I		192.100.9.2	20000	9999	0 ?
* I		192.100.10.2	20000	9999	0 ?
*>I		6.1.5.1	20000	9999	0 ?
* I		6.1.6.1	20000	9999	0 ?
* I		6.1.20.1	20000	9999	0 ?
* I		6.1.20.0/24 192.100.11.2	20000	9999	0 ?
* I		192.100.8.2	20000	9999	0 ?

```
* I      192.100.9.2      20000    9999    0 ?
* I      192.100.10.2    20000    9999    0 ?
Dell#
```

show ip bgp flap-statistics

View flap statistics on BGP routes.

Z9500

Syntax `show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]`

Parameters

- | | |
|----------------------------------|---|
| ipv4 unicast | (OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes. |
| ip-address | (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network. |
| mask | (OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address. |
| filter-list as-path-name | (OPTIONAL) Enter the keyword <code>filter-list</code> then the name of a configured AS-PATH ACL. The range is 140 characters. |
| regexp regular-expression | <p>Enter a regular expression then use one or a combination of the following characters to match. The range is 256 characters.</p> <ul style="list-style-type: none"> • <code>.</code> = (period) any single character (including a white space). • <code>*</code> = (asterisk) the sequences in a pattern (zero or more sequences). • <code>+</code> = (plus) the sequences in a pattern (one or more sequences). • <code>?</code> = (question mark) sequences in a pattern (either zero or one sequences). <p> NOTE: Enter an escape sequence (CTRL+v) prior to entering the <code>?</code> regular expression.</p> <ul style="list-style-type: none"> • <code>[]</code> = (brackets) a range of single-character patterns. • <code>()</code> = (parenthesis) groups a series of pattern elements to a single element. • <code>{ }</code> = (braces) minimum and the maximum match count. • <code>^</code> = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • <code>\$</code> = (dollar sign) the end of the output string. |

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp flap` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

Example

```
Dell>show ip bgp flap-statistics
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
              r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network      From      Flaps      Duration      Reuse
Path
Dell>
```

show ip bgp inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Z9500

Syntax `show ip bgp [ipv4 unicast] inconsistent-as`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp inconsistent-as` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp inconsistent-as
BGP table version is 280852, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, c - confed-external, r -
```

```

redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network Next Hop      Metric LocPrf Weight Path
* 3.0.0.0/8      63.114.8.33              0 18508 209 7018
80 i
*                63.114.8.34              0 18508 209 7018
80 i
*                63.114.8.60              0 18508 209 7018
80 i
*>                63.114.8.33              0 18508 701 80 i
*> 3.18.135.0/24 63.114.8.60              0 18508 209 7018 ?
*                63.114.8.34              0 18508 209 7018 ?
*                63.114.8.33              0 18508 701 7018 ?
*                63.114.8.33              0 18508 209 7018 ?
*> 4.0.0.0/8      63.114.8.60              0 18508 209 1 i
*                63.114.8.34              0 18508 209 1 i
*                63.114.8.33              0 18508 701 1 i
*                63.114.8.33              0 18508 209 1 i
* 6.0.0.0/20      63.114.8.60              0 18508 209 3549 i
*                63.114.8.34              0 18508 209 3549 i
*>                63.114.8.33              0 18508 ?
*                63.114.8.33              0 18508 209 3549 i
* 9.2.0.0/16      63.114.8.60              0 18508 209 701 i
*                63.114.8.34              0 18508 209 701 i
--More--

```

show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.

Z9500

Syntax

```

show ip bgp [ipv4 unicast] neighbors [ip-address [advertised-
routes | dampened-routes | detail | flap-statistics | routes |
{received-routes [network [network-mask]]} | {denied-routes
[network [network-mask]]}]

```

Parameters

<i>ipv4 unicast</i>	(OPTIONAL) Enter the keywords <i>ipv4 unicast</i> to view information only related to ipv4 unicast routes.
<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
<i>advertised-routes</i>	(OPTIONAL) Enter the keywords <i>advertised-routes</i> to view only the routes the neighbor sent.
<i>dampened-routes</i>	(OPTIONAL) Enter the keywords <i>dampened-routes</i> to view information on dampened routes from the BGP neighbor.
<i>detail</i>	(OPTIONAL) Enter the keyword <i>detail</i> to view neighbor-specific internal information for the IPv4 Unicast address family.
<i>flap-statistics</i>	(OPTIONAL) Enter the keywords <i>flap-statistics</i> to view flap statistics on the neighbor's routes.

routes	(OPTIONAL) Enter the keyword <code>routes</code> to view only the neighbor's feasible routes.
received-routes [network [network-mask]	(OPTIONAL) Enter the keywords <code>received-routes</code> then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors.
 NOTE: Configure the <code>neighbor soft-reconfiguration inbound</code> command prior to viewing all the information received from the neighbors.	
denied-routes [network [network-mask]	(OPTIONAL) Enter the keywords <code>denied-routes</code> then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Added the <code>detail</code> option. Output now displays the default MED value.
7.2.1.0	Added the <code>received</code> and <code>denied route</code> options.
6.3.10	The output is changed to display the total number of advertised prefixes.

Usage Information

After a peer reset, the contents of the notification log messages is displayed in hex values for debugging.

The following describes the `show ip bgp neighbors` command shown in the following examples.

The Lines Beginning with:	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays the IPv4 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes the router accepts and the amount of memory used to process those prefixes.

The Lines Beginning with:	Description
Prefix advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

**Example
(S4810 S4820T)**

```
Dell#show ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 23456, external link
  BGP version 4, remote router ID 10.10.10.1
  BGP state ESTABLISHED, in this state for 00:00:35
. . .
Capabilities received from neighbor for IPv4 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  4_OCTECT_AS(65)
  ADD_PATH(69)
  CISCO_ROUTE_REFRESH(128)
```

Example

```
Dell#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv4 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv4 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  ROUTE_REFRESH(2)
```

```
GRACEFUL_RESTART(64)
CISCO_ROUTE_REFRESH(128)
```

```
Route map for incoming advertisements is test
Maximum prefix set to 4 with threshold 75
```

```
For address family: IPv4 Unicast
BGP table version 34, neighbor version 34
5 accepted prefixes consume 20 bytes
Prefix advertised 0, denied 4, withdrawn 0
```

```
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
```

```
Connections established 2; dropped 1
Last reset 00:18:21, due to Maximum prefix limit reached
```

**Example
(Advertised-
Routes)**

```
Dell>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed,
n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next      Hop          Metric LocPrf  Weight Path
*>r 1.10.1.0/24    0.0.0.0           5000                32768 ?
*>r 1.11.0.0/16    0.0.0.0           5000                32768 ?
.....
...
*>I 223.94.249.0/24 223.100.4.249    0             100             0 ?
*>I 223.94.250.0/24 223.100.4.250    0             100             0 ?
*>I 223.100.0.0/16  223.100.255.254 0             100             0 ?
Total number of prefixes: 74102
```

**Example
(Received-
Routes)**

```
BGP table version is 13, local router ID is 120.10.10.1
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network      Next Hop          Metric LocPrf  Weight Path
D  70.70.21.0/24 100.10.10.2          0      0 100 200 ?
D  70.70.22.0/24 100.10.10.2          0      0 100 200 ?
D  70.70.23.0/24 100.10.10.2          0      0 100 200 ?
D  70.70.24.0/24 100.10.10.2          0      0 100 200 ?
*> 70.70.25.0/24 100.10.10.2          0      0 100 200 ?
*> 70.70.26.0/24 100.10.10.2          0      0 100 200 ?
*> 70.70.27.0/24 100.10.10.2          0      0 100 200 ?
*> 70.70.28.0/24 100.10.10.2          0      0 100 200 ?
*> 70.70.29.0/24 100.10.10.2          0      0 100 200 ?
Dell#
```

**Example
(denied-routes)**

```
Dell#show ip bgp neighbors 100.10.10.2 denied-routes
4 denied paths using 205 bytes of memory
BGP table version is 34, local router ID is 100.10.10.2
Status codes: s suppressed, S stale, d damped, h history, *
```

```

valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network      Next Hop      Metric LocPrf Weight Path
D  70.70.21.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.22.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.23.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.24.0/24    100.10.10.2              0      0 100 200 ?
Dell#

```

Related Commands [show ip bgp](#) — views the current BGP routing table.

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Z9500

Syntax `show ip bgp next-hop`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp next-hop` command shown in the following example.

Field	Description
Next-hop	Displays the next-hop IP address.

Field	Description
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	Displays the time elapsed since the next hop was learned. If the route is down, this field displays time elapsed since the route went down.

Example

```
Dell>show ip bgp next-hop
  Next-hop      Via                               RefCount Cost  Flaps  Time
Elapsed
  63.114.8.33 63.114.8.33, Te 2/22    240984   0     0  00:18:25
  63.114.8.34 63.114.8.34, Te 2/22    135152   0     0  00:18:13
  63.114.8.35 63.114.8.35, Te 2/22     1       0     0  00:18:07
  63.114.8.60 63.114.8.60, Te 2/22    135155   0     0  00:18:11
Dell>
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

Z9500

Syntax

```
show ip bgp paths [regexp regular-expression]
```

Parameters

regexp *regular-expression*

Enter a regular expression then use one or a combination of the following characters to match:

- . = (period) any single character (including a white space).
- * = (asterisk) the sequences in a pattern (zero or more sequences).
- + = (plus) the sequences in a pattern (one or more sequences).
- ? = (question mark) sequences in a pattern (either zero or one sequences).



NOTE: Enter an escape sequence (CTRL+v) prior to entering the ? regular expression.

- [] = (brackets) a range of single-character patterns.
- () = (parenthesis) groups a series of pattern elements to a single element.
- { } = (braces) minimum and the maximum match count.
- ^ = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- \$ = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp path` command shown in the following example.

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.
Metric	Displays the MED attribute for this path attribute.
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
Dell#show ip bgp path
Total 16 Paths
Address      Hash Refcount  Metric Path
0x1efe7e5c   15      10000         32 ?
0x1efe7e1c   71      10000         23 ?
0x1efe7ddc  127      10000         22 ?
0x1efe7d9c  183      10000         43 ?
0x1efe7d5c  239      10000         42 ?
0x1efe7c9c  283         6         {102 103} ?
0x1efe7b1c  287      336 20000         ?
0x1efe7d1c  295      10000         13 ?
0x1efe7c5c  339         6         {92 93} ?
0x1efe7cdc  351      10000         12 ?
0x1efe7c1c  395         6         {82 83} ?
0x1efe7bdc  451         6         {72 73} ?
0x1efe7b5c  491      78          0 ?
```

```

0x1efe7adc 883 2 120 i
0x1efe7e9c 983 10000 33 ?
0x1efe7b9c 1003 6 0 i
Dell#

```

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

Z9500

Syntax `show ip bgp paths as-path`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp paths as-path` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these AS-Paths.
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```

Dell#show ip bgp paths as-path
Total 13 AS-Paths
Address      Hash  Refcount  AS-Path
0x1ea3c1ec  251      1      42
0x1ea3c25c  251      1      22

```

```

0x1ea3c1b4 507 1 13
0x1ea3c304 507 1 33
0x1ea3c10c 763 1 {92 93}
0x1ea3c144 763 1 {102 103}
0x1ea3c17c 763 1 12
0x1ea3c2cc 763 1 32
0x1ea3c09c 764 1 {72 73}
0x1ea3c0d4 764 1 {82 83}
0x1ea3c224 1019 1 43
0x1ea3c294 1019 1 23
0x1ea3c02c 1021 4
Dell#

```

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Z9500

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp paths community` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.

Field	Description
Community	Displays the community attributes in this BGP path.

Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address      Hash      Refcount  Community
0x1ec88a5c    3          4 209:209 209:6059 209:31272
3908:900 19092:300
0x1e0f10ec    15         4 209:209 209:3039 209:31272
3908:900 19092:300
0x1c902234    37         2 209:209 209:7193 209:21362
3908:900 19092:300
0x1f588cd4    41        24 209:209 209:6253 209:21362
3908:900 19092:300
0x1e805884    46         2 209:209 209:21226 286:777
286:3033 1899:3033
64675:21092
0x1e433f4c    46         8 209:209 209:5097 209:21362
3908:900 19092:300
0x1f173294    48        16 209:209 209:21226 286:40 286:777
286:3040 5606:40
12955:5606
0x1c9f8e24    50         6 209:209 209:4069 209:21362
3908:900 19092:300
0x1c9f88e4    53         4 209:209 209:3193 209:21362
3908:900 19092:300
0x1f58a944    57         6 209:209 209:2073 209:21362
3908:900 19092:300
0x1ce6be44    80         2 209:209 209:999 209:40832
0x1c6e2374    80         2 209:777 209:41528
0x1f58ad6c    82        46 209:209 209:41528
0x1c6e2064    83         2 209:777 209:40832
0x1f588ecc    85       570 209:209 209:40832
0x1f57cc0c    98         2 209:209 209:21226 286:3031
13646:1044 13646:1124
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204
13646:1214 13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac    117         6 209:209 209:999 209:31272
0x1f5854ac    119        18 209:209 209:21226 286:108 286:111
286:777 286:3033
517:5104
```

show ip bgp peer-group

Allows you to view information on the BGP peers in a peer group.

Z9500

Syntax `show ip bgp [ipv4 unicast] peer-group [peer-group-name] [detail | summary]`

Parameters

ipv4 unicast (OPTIONAL) Enter the keywords *ipv4 unicast* to view information only related to *ipv4 unicast* routes.

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view status information of the peers in that peer group. The output is the same as that found in the <code>show ip bgp summary</code> command.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp peer-group` command shown in the following example.

Line beginning with:	Description
Peer-group	Displays the peer group's name.
Administratively shut	Displays the peer group's status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.
For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.

Line beginning with:	Description
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

Example

```
Dell#show ip bgp peer-group

Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
 12.1.1.2*
 12.1.1.3*
 12.1.1.4*
 12.1.1.5*
 12.1.1.6*
 12.2.1.2*
 12.2.1.3*
 12.2.1.4*
 12.2.1.5*
 12.2.1.6*
 12.3.1.2*
 12.3.1.3*
 12.3.1.4*
 12.3.1.5*
 12.3.1.6*
 12.4.1.2*
 12.4.1.3*
 12.4.1.4*
 12.4.1.5*
 12.4.1.6*
```

Related Commands

[neighbor peer-group \(assigning peers\)](#) — assigns a peer to a peer-group.

[neighbor peer-group \(creating group\)](#) — creates a peer group.

show ip bgp regexp

Display the subset of the BGP routing table matching the regular expressions specified.

Z9500

Syntax

```
show ip bgp regexp regular-expression [character]
```

Parameters

regular-expression
[character]

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (zero or more sequences).
- `+` = (plus) the sequences in a pattern (one or more sequences).
- `?` = (question mark) sequences in a pattern (either zero or one sequences).



NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.

- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp regexp` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.

Field	Description
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

Example (S4810)

```
Dell#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, *
valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      Next Hop      Metric LocPrf Weight Path
*>I 3.0.0.0/8      1.1.1.2          0 100          0 2914 1239 80
i
*>I 4.0.0.0/8      1.1.1.2          0 100          0 2914 3356 i
*>I 4.17.225.0/24  1.1.1.2          0 100          0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.226.0/23  1.1.1.2          0 100          0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.251.0/24  1.1.1.2          0 100          0 2914 11853
11853 11853 11853 11853 6496
*>I 4.17.252.0/23  1.1.1.2          0 100          0 2914 11853
11853 11853 11853 11853 6496
*>I 4.19.2.0/23    1.1.1.2          0 100          0 2914 701
6167 6167 6167 i
*>I 4.19.16.0/23   1.1.1.2          0 100          0 2914 701
6167 6167 6167 i
*>I 4.21.80.0/22   1.1.1.2          0 100          0 2914 174
4200 16559 i
*>I 4.21.82.0/24   1.1.1.2          0 100          0 2914 174
4200 16559 i
*>I 4.21.252.0/23  1.1.1.2          0 100          0 2914 701
6389 8063 19198 i
*>I 4.23.180.0/24  1.1.1.2          0 100          0 2914 3561
6128 30576 i
*>I 4.36.200.0/21  1.1.1.2          0 100          0 2914 14742
11854 14135 i
*>I 4.67.64.0/22   1.1.1.2          0 100          0 2914 11608
19281 i
*>I 4.78.32.0/21   1.1.1.2          0 100          0 2914 3491
29748 i
*>I 6.1.0.0/16     1.1.1.2          0 100          0 2914 701 668
i
*>I 6.2.0.0/22     1.1.1.2          0 100          0 2914 701 668
i
*>I 6.3.0.0/18     1.1.1.2          0 100          0 2914 701 668
i
```

show ip bgp summary

Allows you to view the status of all BGP connections.

Z9500

Syntax `show ip bgp [ipv4 unicast] summary`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp summary` command shown in the following example.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.

Field	Description
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The <code>show ip bgp community</code> command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word <code>never</code> is displayed.

The output format is:

Time Established	Display Example
< 1 day	00:12:23 (hours:minutes:seconds)
< 1 week	1d21h (DaysHours)
> 1 week	11w2d (WeeksDays)

State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the <code>neighbor maximum-prefix</code> command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between
--------------	--

Field	Description
	states and clearing the routes received, the phrase (Purging) may appear in this column.
	If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example (S4810)

```
Dell#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
BGP table version is 34, main routing table version 34
9 network entrie(s) using 1372 bytes of memory
5 paths using 380 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entrie(s) using 168 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
1 BGP community entrie(s) using 43 bytes of memory
2 neighbor(s) using 7232 bytes of memory

Neighbor    AS   MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/
Pfx
100.10.10.2 200    46      41      34    0    0 00:14:33    5
120.10.10.2 300    40      47      34    0    0 00:37:10    0
Dell#
```

show running-config bgp

To display the current BGP configuration, use this feature.

Z9500

Syntax	show running-config bgp
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced on the E-Series.

timers bgp

Adjust the BGP Keep Alive and Hold Time timers.

Z9500

Syntax `timers bgp keepalive holdtime`
To return to the default, use the `no timers bgp` command.

Parameters

<i>keepalive</i>	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is 60 seconds .
<i>holdtime</i>	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is 180 seconds .

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs). MBGP on the Dell Networking OS is implemented as per IETF RFC 1858.

BGPv4 is supported in the following:

Dell Networking OS Version	Platform Support
	Z9500
7.8.1.0, MBGP for IPv6	TeraScale and C-Series
7.8.1.0, MBGP for IPv4 Multicast Only	S-Series
8.2.1.0, MBGP	E-Series ExaScale

debug ip bgp dampening

View information on routes being dampened.

Z9500

Syntax	<pre>debug ip bgp ipv4 multicast dampening</pre> To disable debugging, use the <code>no debug ip bgp ipv4 multicast dampening</code> command.	
Parameters	dampening	Enter the keyword <code>dampening</code> to clear route flap dampening information.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced IPv6 MGBP support for the E-Series.

distance bgp

Configure three administrative distances for routes.

Z9500

Syntax `distance bgp external-distance internal-distance local-distance`
To return to default values, use the `no distance bgp` command.

Parameters	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is 20 .
	<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is 200 .
	<i>local-distance</i>	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is 200 .

Defaults	• external-distance = 20
	• internal-distance = 200
	• local-distance = 200

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information  **CAUTION: Dell Networking recommends not changing the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.**

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

**Related
Commands**

[router bgp](#) — enters ROUTER mode on the switch.

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Z9500

Syntax

```
show ip bgp [ipv4 unicast] dampened-paths
```

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

**Usage
Information**

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      From      Reuse      Path
Dell>
```

BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute.

BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new "Type" field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

deny

To reject (deny) from the two types of extended communities, route origin (rt) or site-of-origin (soo), use this feature.

Z9500

Syntax

```
deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}
```

To remove (delete) the rule, use the `no deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}` command.

Parameters

rt	Enter the keyword <code>rt</code> to designate a Route Origin community.
soo	Enter the keyword <code>soo</code> to designate a Site-of-Origin community (also known as Route Origin).
as4 ASN4:NN	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).

Defaults

Not configured.

Command Modes	CONFIGURATION (conf-ext-community-list)										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.	7.6.1.0	Introduced on the E-Series.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
7.8.1.0	Introduced on the S-Series.										
7.7.1.0	Introduced on the C-Series.										
7.6.1.0	Introduced on the E-Series.										
Related Commands	permit — configures to add (permit) rules. show ip extcommunity-list — displays the extended community list.										

deny regex

This feature allows you to specify an extended community to reject (deny) using a regular expression (regex).

Z9500

Syntax	<pre>deny regex {regex}</pre> To remove, use the <code>no deny regex {regex}</code> command.										
Parameters	<table> <tr> <td>regex</td><td>Enter a regular expression.</td></tr> </table>	regex	Enter a regular expression.								
regex	Enter a regular expression.										
Defaults	Not configured.										
Command Modes	CONFIGURATION (conf-ext-community-list)										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.	7.6.1.0	Introduced on the E-Series.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
7.8.1.0	Introduced on the S-Series.										
7.7.1.0	Introduced on the C-Series.										
7.6.1.0	Introduced on the E-Series.										

Usage Information	Duplicate commands are silently accepted.
Example	<pre>Dell(conf-ext-community-list)#deny regexp 123 Dell(conf-ext-community-list)#</pre>
Related Commands	permit regex — permits a community using a regular expression.

description

To designate a meaningful description to the extended community, use this feature.

Z9500

Syntax	<pre>description {line}</pre> To remove the description, use the <code>no description {line}</code> command.
Parameters	line Enter a description (maximum 80 characters).
Defaults	Not configured.
Command Modes	CONFIGURATION (conf-ext-community-list)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

ip extcommunity-list

To enter the Extended Community-list mode, use this feature.

Z9500

Syntax	<pre>ip extcommunity-list word</pre> To exit from this mode, use the <code>exit</code> command.
Parameters	word Enter a community list name (maximum 16 characters).

Defaults	none										
Command Modes	CONFIGURATION (conf-ext-community-list)										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.	7.6.1.0	Introduced on the E-Series.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
7.8.1.0	Introduced on the S-Series.										
7.7.1.0	Introduced on the C-Series.										
7.6.1.0	Introduced on the E-Series.										
Usage Information	This mode changes the prompt.										
Example	<pre>Dell(conf)#ip extcommunity-list test Dell(conf-ext-community-list)#</pre>										

match extcommunity

To match an extended community in the Route Map mode, use this feature.

Z9500

Syntax	<pre>match extcommunity {extended community list name}</pre> To change the match, use the <code>no match extcommunity {extended community list name}</code> command.				
Parameters	<table> <tr> <td><i>extended community list name</i></td><td>Enter the name of the extended community list.</td></tr> </table>	<i>extended community list name</i>	Enter the name of the extended community list.		
<i>extended community list name</i>	Enter the name of the extended community list.				
Defaults	none				
Command Modes	ROUTE MAP (config-route-map)				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				

	Version	Description
	7.8.1.0	Introduced on the S-Series.
	7.7.1.0	Introduced on the C-Series.
	7.6.1.0	Introduced on the E-Series.
Usage Information	Like standard communities, you can use extended communities in the route-map to match the attribute.	
Example	<pre>Dell(config-route-map)#match extcommunity Freedombird Dell(config-route-map)#</pre>	

permit

To add rules (permit) from the two types of extended communities, Route Origin (rt) or Site-of-Origin (soo), use this feature.

Z9500

Syntax	<pre>permit {rt soo} {as4 ASN4:NN ASN:NNNN IPADDR:NN}</pre> To change the rules, use the <code>no permit {rt soo} {as4 ASN4:NN ASN:NNNN IPADDR:NN}</code> command.	
Parameters	rt	Enter the keyword <code>rt</code> to designate a Route Origin community.
	soo	Enter the keyword <code>soo</code> to designate a Site-of-Origin community (also known as Route Origin).
	as4 ASN4:NN	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).
	ASN:NNNN	Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).
	IPADDR:NN	Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).
Defaults	Not configured.	
Command Modes	CONFIGURATION (conf-ext-community-list)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Related Commands

[deny](#) — configures to delete (deny) rules.

[show ip bgp extcommunity-list](#) — displays the extended community list.

permit regex

This feature allows you specify an extended community to forward (permit) using a regular expression (regex).

Z9500

Syntax

```
permit regex {regex}
```

To remove, use the `no permit regex {regex}` command.

Parameters

regex Enter a regular expression.

Defaults

Not configured.

Command Modes

CONFIGURATION (conf-ext-community-list)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

Duplicate commands are silently accepted.

Example

```
Dell(conf-ext-community-list)#permit regexp 123
Dell(conf-ext-community-list)#
```

Related
Commands

[deny regex](#) — denies a community using a regular expression.

set extcommunity rt

To set Route Origin community attributes in Route Map, use this feature.

Z9500

Syntax

```
set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]
```

To delete the Route Origin community, use the `no set extcommunity` command.

Parameters

as4 ASN4:NN	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
additive	(OPTIONAL) Enter the keyword <code>additive</code> to add to the existing extended community.
non-trans	(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.

Defaults

none

Command Modes

ROUTE MAP (config-route-map)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T
8.3.11.1	Introduced on the Z-9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.6.1.0	Introduced on the E-Series.
Version	Description				
7.6.1.0	Introduced on the E-Series.				
Usage Information	If the set community <code>rt</code> and <code>soo</code> are in the same route-map entry, the behavior defines as: • If the <code>rt</code> option comes before <code>soo</code>, with or without the <code>additive</code> option, <code>soo</code> overrides the communities <code>rt</code> sets. • If the <code>rt</code> option comes after <code>soo</code>, without the <code>additive</code> option, <code>rt</code> overrides the communities <code>soo</code> sets. • If the <code>rt</code> with the <code>additive</code> option comes after <code>soo</code>, <code>rt</code> adds the communities <code>soo</code> sets.				
Related Commands	set extcommunity soo — sets the extended community site-of-origin in the route-map.				

set extcommunity soo

To set extended community site-of-origin in Route Map, use this feature.

Z9500

Syntax	<pre>set extcommunity soo {as4 ASN4:NN ASN:NNNN IPADDR:NN [non-trans]}</pre> To delete the site-of-origin community, use the <code>no set extcommunity</code> command.								
Parameters	<table> <tr> <td>as4 ASN4:NN</td><td>Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).</td></tr> <tr> <td>ASN:NNNN</td><td>Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).</td></tr> <tr> <td>IPADDR:NN</td><td>Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).</td></tr> <tr> <td>non-trans</td><td>(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.</td></tr> </table>	as4 ASN4:NN	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).	ASN:NNNN	Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).	IPADDR:NN	Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).	non-trans	(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.
as4 ASN4:NN	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).								
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).								
IPADDR:NN	Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).								
non-trans	(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.								
Defaults	none								
Command Modes	ROUTE MAP (config-route-map)								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.								

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

Related Commands

[set extcommunity rt](#) — sets the extended community route origins using the route-map.

show ip bgp ipv4 extcommunity-list

To display the IPv4 routes matching the extended community list name, use this feature.

Z9500

Syntax

```
show ip bgp [ipv4 [multicast | unicast] | ipv6 unicast]
extcommunity-list name
```

Parameters

multicast	Enter the keyword <code>multicast</code> to display the multicast route information.
unicast	Enter the keyword <code>unicast</code> to display the unicast route information.
ipv6 unicast	Enter the keywords <code>ipv6 unicast</code> to display the IPv6 unicast route information.
<i>name</i>	(OPTIONAL) Enter the name of the extcommunity-list.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

If there is a type or sub-type that is not well-known, it is displayed as:TTSS:XX:YYYY.

Where TT is type, SS is sub-type displayed in hexadecimal format, XX:YYYY is the value divided into 2-byte and 4-byte values in decimal format. This format is consistent with other vendors.

For example, if the extended community has type 0x04, sub-type 0x05, value 0x20 00 00 00 10 00, it displays as:0x0405:8192:4096.

Non-transitive extended communities are marked with an asterisk.

Example

```
Dell#show ip bgp ipv4 multicast extcommunity-list
BGP routing table entry for 192.168.1.0/24, version 2

Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from :
  100.100.1.2 (2.4.0.1) Best
    AS_PATH : 200
    Next-Hop : 100.100.1.2, Cost : 0
    Origin IGP, Metric 4294967295 (Default), LocalPref 100,
Weight 0,
external
  Communities :
    300:400 500:600

    Extended Communities :
    RT:1111:4278080 SoO:35:4 SoO:36:50529043 SoO:37:50529044
    SoO:38:50529045 SoO:0.0.0.2:33 SoO:506.62106:34
0x0303:254:11223*

Dell#
```

show ip bgp paths extcommunity

To display all BGP paths having extended community attributes, use this feature.

Z9500

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information The following describes the `show ip bgp paths extcommunity` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
RefCount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

Example

```
Dell#show ip bgp paths extcommunity
Total 1 Extended Communities

Address      Hash  Refcount  Extended Community
0x41d57024  12272  1          RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

Dell#
```

show ip extcommunity-list

Display the IP extended community list.

Z9500

Syntax	show ip extcommunity-list [word]	
Parameters	word	Enter the name of the extended community list you want to view.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example

```
Dell#show ip extcommunity-list test
ip extcommunity-list test
  deny RT:1234:12
  permit regexp 123
  deny regexp 234
  deny regexp 123
Dell#
```

show running-config extcommunity-list

To display the current configuration of the extended community lists, use this feature.

Z9500

Syntax	show running-config extcommunity-list [word]	
Parameters	word	Enter the name of the extended community list you want to view.

Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example

```
Dell#show running-config extcommunity-list test

ip extcommunity-list test
  permit rt 65033:200
  deny soo 101.11.11.2:23
  permit rt as4 110212:340
  deny regex ^(65001_)$

Dell#
```

IPv6 BGP Commands

IPv6 border gateway protocol (IPv6 BGP) is an external gateway protocol that transmits interdomain routing information with extended IP address space within and between Autonomous Systems (AS). Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

address-family

Enable the IPv4 multicast or the IPv6 address family.

Z9500

Syntax	address-family [ipv4 multicast ipv6unicast]	
Parameters	ipv4multicast	Enter BGPv4 multicast mode.
	ipv6unicast	Enter BGPv6 mode.
Defaults	Not configured.	

Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	6.5.1.0	Introduced
Usage Information	Enter <code>ipv6unicast</code> to enter the BGP for IPv6 mode (CONF-ROUTER_BGPv6_AF).	

address family ipv6 unicast

This command changes the context to subsequent address family identifier (SAFI).

Z9500

Syntax	<code>address family ipv6 unicast</code>	
	To remove SAFI context, use the <code>no address family ipv6 unicast</code> command.	
Parameters	ipv6	Enter the keyword <code>ipv6</code> to specify the address family as IPv6.
	unicast	Enter the keyword <code>unicast</code> to specify multicast as SAFI.
Defaults	IPv6 Unicast	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced
Usage Information	All subsequent commands apply to this address family after you execute this command. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering <code>exit</code> and returning to the Router BGP context.	

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

Z9500

Syntax	<code>aggregate-address ipv6-address prefix-length [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]</code>
---------------	---

Parameters

***ipv6-address
prefix-length***

Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

***advertise-map
map-name***

(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.

as-set

(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate.

AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

***attribute-map
map-name***

(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.

summary-only

(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes will not be advertised.

***suppress-map
map-name***

(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

CONFIGURATION-ROUTER-BGPV6-ADDRESS FAMILY

Command History

Version

Description

9.2(1.0)

Introduced on the Z9500.

8.2.1.0

Introduced on the E-Series ExaScale.

7.4.1.0

Introduced

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected via the network command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Z9500

Syntax

`bgp always-compare-med`

To disable comparison of MED, use the `no bgp always-compare-med` command.

Defaults

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes

ROUTER BGP

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage

Information

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

Z9500

Syntax

`bgp bestpath as-path ignore`

To return to the default, use the `no bgp bestpath as-path ignore` command.

Defaults	Disabled (that is, the software considers the AS_PATH when choosing a route as best).	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.	

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Z9500

Syntax	<code>bgp bestpath med confed</code> To disable MED comparison on BGP confederation paths, use the <code>no bgp bestpath med confed</code> command.	
Defaults	Disabled	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.	

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Z9500

Syntax	<code>bgp bestpath med missing-as-best</code>	
	To return to the default selection, use the <code>no bgp bestpath med missing-as-best</code> command.	
Defaults	Disabled	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.	

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

Z9500

Syntax	<code>bgp client-to-client reflection</code>	
	To disable client-to-client reflection, use the <code>no bgp client-to-client reflection</code> command.	
Defaults	Enabled when a route reflector is configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Usage Information Route reflection to clients is not necessary if all client routers are fully meshed.

- Related Commands**
- [bgp cluster-id](#) – assigns an ID to a BGP cluster with two or more route reflectors.
 - [neighbor route-reflector-client](#) – configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Z9500

Syntax `bgp cluster-id {ip-address | number}`
To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

<i>ip-address</i>	Enter an IP address as the route reflector cluster ID.
<i>number</i>	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Usage Information When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the `cluster-id` as an integer, it is displayed as an integer.

- Related Commands**
- [bgp client-to-client reflection](#) – enables route reflection between route reflector and clients.
 - [neighbor route-reflector-client](#) – configures a route reflector and clients.
 - [show ip bgp cluster-list](#) – views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

Z9500

Syntax	<code>bgp confederation identifier as-number</code>	
	To delete a BGP confederation identifier, use the <code>no bgp confederation identifier as-number</code> command.	
Parameters	<i>as-number</i>	Enter the AS number. The range is 1 to 65535.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The autonomous systems configured in this command are visible to the EBGp neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.	
	The system accepts confederation EBGp peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.	

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

Z9500

Syntax	<code>bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]</code>	
	To disable route dampening, use the <code>no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]</code> command.	
Parameters	<i>half-life</i>	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the

	half-life period expires. The range is 1 to 45. The default is 15 minutes .	
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is 1 to 20000. The default is 750 .	
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is 1 to 20000. The default is 2000 .	
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is 1 to 255. The default is 60 minutes .	
route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> followed by the name of a configured route map. Only match commands in the configured route map are supported.	
Defaults	Disabled.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you enter <code>bgp dampening</code> , the default values for <i>half-life</i> , <i>reuse</i> , <i>suppress</i> , and <i>max-suppress-time</i> are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.	
Related Commands	show ip bgp dampened-paths – views the BGP paths.	

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

Z9500

Syntax	<code>bgp default local-preference value</code> To return to the default value, use the <code>no bgp default local-preference</code> command.
---------------	--

Parameters	value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is 0 to 4294967295. The default is 100 .
Defaults	100	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The <code>bgp default local-preference</code> command setting is applied by all routers within the AS.	

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGp peers.

Z9500

Syntax	<code>bgp enforce-first-as</code> To turn off the default, use the <code>no bgp enforce-first-as</code> command.	
Defaults	Enabled.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	This is enabled by default, that is for all updates received from EBGp peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the <code>show ip bgp neighbors</code> command to view the “failed enforce-first-as check” counter. If you disable enforce-first-as, you can view it using the <code>show ip protocols</code> command.	

**Related
Commands**

- [show ip bgp neighbors](#) – views the information exchanged by BGP neighbors.
- [show ip protocols](#) – views information on routing protocols.

bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Z9500

Syntax	<code>bgp fast-external-fallover</code> To disable fast external fallover, use the <code>no bgp fast-external-fallover</code> command.	
Defaults	Enabled.	
Command Modes	ROUTER BGP	
Command History	Version 9.2(1.0)	Introduced on the Z9500.
	Version 8.2.1.0	Introduced on the E-Series ExaScale.
	Version 7.4.1.0	Introduced
Usage Information	The <code>bgp fast-external-fallover</code> command appears in the <code>show config</code> command output.	

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

Z9500

Syntax	<code>bgp four-octet-as-support</code> To disable fast external fallover, use the <code>no bgp four-octet-as-support</code> command.	
Defaults	Disabled (supports 2-Byte format).	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced

Usage Information

Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router is slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4- or 2-byte identified routers. You cannot mix them.

Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements will reflect the entered format.

For more information about using the 2- or 4-Byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Z9500

Syntax

```
bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]
```

To return to the default, use the `no bgp graceful-restart` command.

Parameters

neighbor ip-address | peer-group-name

Enter the keyword `neighbor` followed by one of the options listed below:

- `ip-address` of the neighbor in IP address format of the neighbor.
- `peer-group-name` of the neighbor peer group.

restart-time seconds

Enter the keywords `restart-time` followed by the maximum number of seconds needed to restart and bring up all peers. The range is 1 to 3600 seconds. The default is **120 seconds**.

stale-path-time seconds

Enter the keywords `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.

role receiver-only

Enter the keywords `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults

As above.

Command Modes

ROUTER BGP

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.	

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

Z9500

Syntax	<code>bgp log-neighbor-changes</code>	
	To disable logging, use the <code>no bgp log-neighbor-changes</code> command.	
Defaults	Enabled.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The <code>bgp log-neighbor-changes</code> command appears in the <code>show config</code> command output.	
Related Commands	show config – views the current configuration.	

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

Z9500

Syntax	<code>bgp non-deterministic-med</code>	
	To return to the default, use the <code>no bgp non-deterministic-med</code> command.	
Defaults	Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).	

Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (<code>no bgp non-deterministic-med</code>), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS. When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter the <code>clear ip bgp</code> command to clear existing paths.	

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

Z9500

Syntax	<code>bgp recursive-bgp-next-hop</code> To disable next-hop resolution, use the <code>no bgp recursive-bgp-next-hop</code> command.	
Defaults	Enabled.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	This command is a <i>knob</i> to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.	

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

**Related
Commands** [clear ip bgp](#)

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

Z9500

Syntax	bgp regex-eval-optz-disable To re-enable optimization engine, use the no bgp regex-eval-optz-disable command.									
Defaults	Enabled.									
Command Modes	ROUTER BGP (conf-router_bgp)									
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.2.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced	
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.2.1.0	Introduced on the E-Series ExaScale.									
7.6.1.0	Introduced									
Usage Information	BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines. BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the show bgp commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The regex engine performance enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.									
Related Commands	show ip protocols – views information on all enabled and active routing protocols.									

bgp router-id

Assign a user-given ID to a BGP router.

Z9500

Syntax	<code>bgp router-id ip-address</code> To delete a user-assigned IP address, use the <code>no bgp router-id</code> command.									
Parameters	<i>ip-address</i>	Enter an IP address in dotted decimal format to reset only that BGP neighbor.								
Defaults	The router ID is the highest IP address of the Loopback interface or, if you do not configure Loopback interfaces, the highest IP address of a physical interface on the router.									
Command Modes	ROUTER BGP									
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.4.1.0</td><td>Introduced</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.2.1.0	Introduced on the E-Series ExaScale.	7.4.1.0	Introduced	
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.2.1.0	Introduced on the E-Series ExaScale.									
7.4.1.0	Introduced									
Usage Information	Peering sessions are reset when you change the router ID of a BGP router.									

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

Z9500

Syntax	<code>bgp soft-reconfig-backup</code> To return to the default setting, use the <code>no bgp soft-reconfig-backup</code> command.	
Defaults	Off	
Command Modes	ROUTER BGP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

Usage Information

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

Related Commands

[clear ip bgp](#) — activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Z9500

Syntax `capture bgp-pdu max-buffer-size 100-102400000`

Parameters

100-102400000	Enter a size for the capture buffer.
0	

Defaults **40960000 bytes**

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced

Related
Commands

- [show capture bgp-pdu neighbor](#) – configures a route reflector and clients.
- [capture bgp-pdu neighbor](#) – enables capture of an IPv4 BGP neighbor packet.

capture bgp-pdu neighbor (ipv6)

Enable capture of an IPv6 BGP neighbor packet.

Z9500

Syntax

```
capture bgp-pdu neighbor ipv6-address direction {both | rx | tx}
```

To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

Parameters

<i>ipv6-address</i>	Enter the IPv6 address of the target BGP neighbor.
direction {both rx tx}	Enter the keyword <code>direction</code> and a direction— either <code>rx</code> for inbound, <code>tx</code> for outbound, or <code>both</code> .

Defaults

Not configured.

Command
Modes

- EXEC
- EXEC Privilege

Command
History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced

Related
Commands

- [clear ip bgp](#) – enables route reflection between route reflector and clients.
- [show capture bgp-pdu neighbor](#) – configures a route reflector and clients.
- [capture bgp-pdu neighbor](#) – enables capture of an IPv4 BGP neighbor packet.

clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address. The `soft` parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Z9500

Syntax

```
clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}} | soft [in | out]
```

Parameters

<i>ipv6-address</i>	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword resets all neighbors belonging to that IP.
flap-statistics	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to clear all flap statistics belonging to that AS or a specified address family within that IP.
ipv4	(OPTIONAL) Enter the keyword <code>ipv4</code> to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword <code>ipv6</code> to select options for that address family.
unicast	(OPTIONAL) Enter the keyword <code>unicast</code> to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword <code>multicast</code> to select the multicast option within the selected address family. Multicast is supported on IPv4 only
soft	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
	 NOTE: If you enter <code>clear ip bgp ipv6-address soft</code> , both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
out	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.

Command Modes

EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

clear ip bgp * (asterisk)

Reset all BGP sessions in the specified category. The `soft` parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Z9500

Syntax

```
clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast  
soft [in | out] | soft [in | out]]
```

Parameters	*	Enter an asterisk (*) to reset all BGP sessions.
	ipv4 multicast soft [in out]	(OPTIONAL) This keyword sequence sets options within the a specified IPv4 address family.
	ipv6 unicast soft [in out]	(OPTIONAL) This keyword sequence sets options within the a specified IPv6 address family.
	soft	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
	 NOTE: If you enter <code>clear ip bgp ip6-address soft</code> , both inbound and outbound policies are reset.	
	in	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
Command Modes	out	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.
	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

clear ip bgp as-number

Reset BGP sessions. The `soft` parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Z9500

Syntax	<pre>clear ip bgp as-number [flap-statistics ipv4 {multicast {flap-statistics soft {in out}} unicast {flap-statistics soft {in out}} ipv6 unicast {flap-statistics soft {in out}} soft [in out]</pre>	
Parameters	as-number	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is 1 to 65535.
	flap-statistics	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to clear all flap statistics belonging to that AS or a specified address family within that AS.

	ipv4	(OPTIONAL) Enter the keyword <code>ipv4</code> to select options for that address family.
	ipv6	(OPTIONAL) Enter the keyword <code>ipv6</code> to select options for that address family.
	unicast	(OPTIONAL) Enter the keyword <code>unicast</code> to select the unicast option within the selected address family.
	multicast	(OPTIONAL) Enter the keyword <code>multicast</code> to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
	soft	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
	in	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
	out	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

Z9500

Syntax	<code>clear ip bgp ipv6 unicast dampening [ipv6-address]</code>	
Parameters	ipv6-address	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
Command Modes	EXEC Privilege	

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	After you enter this command, the software deletes history routes and returns suppressed routes to active state.	

clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Z9500

Syntax	<code>clear ip bgp ipv6 unicast flap-statistics [ipv6-address filter-list as-path-name regexp regular-expression]</code>	
Parameters	ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	filter-list as-path-name	(OPTIONAL) Enter the keywords <code>filter-list</code> followed by the name of a configured AS-PATH list.
	regexp regular-expression	(OPTIONAL) Enter the keyword <code>regexp</code> followed by regular expressions. Use one or a combination of the following: . (period) matches on any single character, including white space. * (asterisk) matches on sequences in a pattern (zero or more sequences). + (plus sign) matches on sequences in a pattern (one or more sequences). ? (question mark) matches sequences in a pattern (0 or 1 sequences). [] (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.) \$ (dollar sign) matches the end of the output string.

Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you enter <code>clear ip bgp flap-statistics</code> without any parameters, all statistics are cleared.	
Related Commands	show ip bgp ipv6 unicast flap-statistics – views BGP flap statistics.	

clear ip bgp ipv6 unicast

Reset MBGP sessions.

Z9500

Syntax	<code>clear ip bgp ipv6 unicast * <i>ipv6-address prefix-length</i> [dampening flap-statistics] peer-group</code>	
Parameters	*	Enter the character <code>*</code> to clear all peers.
	<i>ipv6-address prefix-length</i>	Enter the IPv6 address in the <code>x::x:x::x</code> format followed by the prefix length in the <code>/x</code> format. The range is <code>/0</code> to <code>/128</code> .
	 NOTE: The <code>::</code> notation specifies successive hexadecimal fields of zeros.	
	dampening	(OPTIONAL) Enter the keyword <code>dampening</code> to clear route flap dampening information.
	flap-statistics	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to reset the flap statistics on all prefixes from that neighbor.
Command Modes	peer-group	(OPTIONAL) Enter the keywords <code>peer-group</code> to clear all members of a peer-group.
	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

Z9500

Syntax	<code>clear ip bgp dampening ipv6 unicast [<i>network network-mask</i>]</code>	
Parameters	<i>network</i>	(OPTIONAL) Enter the IPv6 network address in x:x:x:x format.
	<i>network-mask</i>	If you enter the network address, then enter the network mask, from 0 to 128.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

clear ip bgp ipv6 unicast flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Z9500

Syntax	<code>clear ip bgp ipv6 unicast flap-statistics [<i>network</i> <i>filter-list list</i> <i>regexp regexp</i>]</code>	
Parameters	<i>network</i>	(OPTIONAL) Enter the IPv6 network address in x:x:x:x format to clear flap statistics.
	<i>filter-list list</i>	(OPTIONAL) Enter the keywords <code>filter-list</code> followed by the name of a configured AS-PATH list A maximum of 16 characters.
	<i>regexp regexp</i>	(OPTIONAL) Enter the keyword <code>regexp</code> followed by regular expressions. Use one or a combination of the following: • <code>.</code> (period) matches on any single character, including white space. • <code>*</code> (asterisk) matches on sequences in a pattern (zero or more sequences). • <code>+</code> (plus sign) matches on sequences in a pattern (one or more sequences). • <code>?</code> (question mark) matches sequences in a pattern (0 or 1 sequences). • <code>[]</code> (brackets) matches a range of single-character patterns.

- ^ (caret) matches the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- \$ (dollar sign) matches the end of the output string.

Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

Z9500

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name]
keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out] command`.

Parameters	ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.
		 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group peer-group-name	(OPTIONAL) Enter the keywords <code>peer-group</code> followed by the name of the peer group.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound keepalive routes.
	out	(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound keepalive routes.

Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	7.4.1.0	Introduced				
Version	Description								
7.4.1.0	Introduced								
Usage Information	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.								
debug ip bgp ipv6 dampening View information on IPv6 routes being dampened. Z9500									
Syntax	<pre>debug ip bgp ipv6 unicast dampening [in out]</pre> To disable debugging, use the <code>no debug ip bgp ipv6 unicast dampening</code> command.								
Parameters	<table> <tr> <td>in</td><td>(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound dampened routes.</td></tr> <tr> <td>out</td><td>(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound dampened routes.</td></tr> </table>	in	(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound dampened routes.	out	(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound dampened routes.				
in	(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound dampened routes.								
out	(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound dampened routes.								
Command Modes	EXEC Privilege								
Command History	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.2.1.0	Introduced on the E-Series ExaScale.	7.4.1.0	Introduced
Version	Description								
9.2(1.0)	Introduced on the Z9500.								
8.2.1.0	Introduced on the E-Series ExaScale.								
7.4.1.0	Introduced								
Usage Information	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.								
Related Commands	show ip bgp dampened-paths – View BGP dampened routes.								

debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

Z9500

Syntax	<pre>debug ip bgp ipv6 unicast peer-group <i>peer-group-name</i> updates [in out]</pre> To disable debugging, use the <code>no debug ip bgp ipv6 unicast peer-group <i>peer-group-name</i> updates [in out]</code> command.
---------------	--

Parameters	peer-group <i>peer-group-name</i>	Enter the keywords <code>peer-group</code> followed by the name of the peer-group.
	updates	Enter the keyword <code>updates</code> to view BGP update information.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.
	out	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

Z9500

Syntax	<code>debug ip bgp ipv6 unicast dampening</code> To disable debugging, use the <code>no debug ip bgp ipv6 unicast dampening</code> command.	
Parameters	dampening	Enter the keyword <code>dampening</code> to clear route flap dampening information.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

debug ip bgp ipv6 unicast updates

View information about BGP updates.

Z9500

Syntax	<pre>debug ip bgp ipv6 unicast <i>ipv6-address prefix-length</i> updates [in out]</pre>	
	To disable debugging, use the <code>no debug ip bgp ipv6 unicast <i>ipv6-address prefix-length</i> updates [in out]</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.
	<i>prefix-length</i>	 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	updates	Enter the keyword <code>updates</code> to view BGP update information.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.
	out	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.
Defaults	Disabled.	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

Z9500

Syntax	<pre>debug ip bgp [<i>ipv6-address</i> peer-group <i>peer-group-name</i>] notifications [in out]</pre>	
	To disable debugging, use the <code>no debug ip bgp [<i>ip-address</i> peer-group <i>peer-group-name</i>] notifications [in out]</code> command.	
Parameters	<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

	peer-group peer-group- name	(OPTIONAL) Enter the keywords <code>peer-group</code> followed by the name of the peer group.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view BGP notifications received from neighbors.
	out	(OPTIONAL) Enter the keyword <code>out</code> to view BGP notifications sent to neighbors.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.	

debug ip bgp updates

Allows you to view information about BGP updates.

Z9500

Syntax	<pre>debug ip bgp [ipv6-address peer-group peer-group-name ipv6 unicast [ipv6-address]] updates [in out prefix-list prefix- list-name]</pre> To disable debugging, use the <code>no debug ip bgp [ip-address peer-group peer-group-name ipv6 unicast [ipv6-address]] updates [in out]</code> command.	
Parameters	ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.
		 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group peer-group- name	(OPTIONAL) Enter the keywords <code>peer-group</code> followed by the name of the peer group.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view BGP updates received from neighbors.

	out	(OPTIONAL) Enter the keyword <code>out</code> to view BGP notifications updates sent to neighbors.
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.	

default-metric

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

Z9500

Syntax	<code>default-metric number</code> To return to the default setting, use the <code>no default-metric</code> command.	
Parameters	<i>number</i>	Enter a number as the metric to be assigned to routes from other protocols. The range is 1 to 4294967295.
Defaults	0	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The <code>default-metric</code> command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.	
Related Commands	• bgp always-compare-med – enables comparison of all BGP MED attributes. • redistribute – redistributes routes from other routing protocols into BGP.	

description

Enter a description of the BGP routing protocol.

Z9500

Syntax	<code>description {description}</code> To remove the description, use the <code>no description {description}</code> command.	
Parameters	<i>description</i>	Enter a description to identify the BGP protocol (80 characters maximum).
Defaults	none	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Related Commands	router bgp – Enter ROUTER mode on the switch.	

distance bgp

Configure three administrative distances for routes.

Z9500

Syntax	<code>distance bgp external-distance internal-distance local-distance</code> To return to default values, use the <code>no distance bgp</code> command.	
Parameters	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is 20 .
	<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is 200 .
	<i>local-distance</i>	Enter a number to assign to routes learned from networks listed in the <code>network</code> command. The range is 1 to 255. The default is 200 .
Defaults	<code>external-distance = 20</code>	

- `internal-distance = 200`
- `local-distance = 200`

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information



CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

ipv6 prefix-list

Configure an IPv6 prefix list.

Z9500

Syntax

`ipv6 prefix-list prefix-list name`

Parameters

prefix-list name Enter the name of the prefix list.



NOTE: There is a 140-character limit for prefix list names.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

Related Commands [show ipv6 prefix-list](#) — View the selected IPv6 prefix-list.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Z9500

Syntax	<code>maximum-paths {ebgp ibgp} number</code>	
	To return to the default values, use the <code>no maximum-paths</code> command.	
Parameters	ebgp	Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.
	ibgp	Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes
	number	Enter a number as the maximum number of parallel paths. The range is 1 to 16. The default is 1 .
Defaults	1	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you enable this command, use the <code>clear ip bgp</code> command to recompute the best path.	

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} activate</code>
	To disable, use the <code>no neighbor {ipv6-address peer-group-name} activate</code> command.

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Identify a peer group by name.
	activate	Enter the keyword activate to enable the identified neighbor or peer group in the new AFI/SAFI.
Defaults	Disabled.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	By default, when you create a neighbor/peer group configuration in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using activate in the new context, the neighbor/peer group is enabled for AFI/SAFI.	

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Z9500

Syntax	<code>neighbor {<i>ipv6-address</i> <i>peer-group-name</i>} advertisement-interval <i>seconds</i></code>
	To return to the default value, use the <code>no neighbor {<i>ipv6-address</i> <i>peer-group-name</i>} advertisement-interval</code> command.

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>seconds</i>	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is 5 seconds for internal BGP peers and 30 seconds for external BGP peers.

Defaults

- *seconds* = **5 seconds** (internal peers)
- *seconds* = **30 seconds** (external peers)

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Z9500

Syntax

`neighbor {ip-address | peer-group-name} allowas-in number`
To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters

<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x::x format.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
<i>number</i>	Enter a number of times to allow this neighbor ID to use the AS path. The range is 1 to 10.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands

[bgp four-octet-as-support](#) – enables 4-Byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Z9500

Syntax	<pre>neighbor {ipv6-address peer-group-name} default-originate [route-map map-name]</pre> To remove a default route, use the <code>no neighbor {ipv6-address peer-group-name} default-originate [route-map map-name]</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>route-map map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> followed by the name of a configured route map.
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you apply a route map to a BGP peer or neighbor with the <code>neighbor default-originate</code> command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.	

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

Z9500

Syntax	<pre>neighbor {ipv6-address peer-group-name} description text</pre> To delete a description, use the <code>no neighbor {ipv6-address peer-group-name} description text</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x:x format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>text</i>	Enter a continuous text string up to 80 characters.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

neighbor distribute-list

Distribute BGP information via an established prefix list.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} distribute-list
prefix-list-name {in | out}
```

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>prefix-list-name</i>	Enter the name of an established prefix list. If you do not configure the prefix list, the default is <code>permit</code> (to allow all routes).
	<i>in</i>	Enter the keyword <code>in</code> to distribute only inbound traffic.
	<i>out</i>	Enter the keyword <code>out</code> to distribute only outbound traffic.
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Other BGP filtering commands include the <code>neighbor filter-list</code> and <code>neighbor route-map</code> commands.	
Related Commands	• neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group. • neighbor route-map – assigns a route map to a neighbor or peer group.	

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]
```

To disallow and disconnect connections, use the `no neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]` command.

Parameters

<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x::x format.
	 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>ttl</i>	(OPTIONAL) Enter the number of hops as the time to live (ttl) value. The range is 1 to 255. The default is 255 .

Defaults Disabled.

Command Modes ROUTER BGP

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Usage Information

To prevent loops, the `neighbor ebgp-multihop` command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} fall-over</code>	
	To disable, use the <code>no neighbor {ipv6-address peer-group-name} fall-over</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group.
Defaults	Disabled.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	When you enable fall-over, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.	
Related Commands	show ip bgp neighbors – displays information on the BGP neighbors.	

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} filter-list as-path-name {in out}</code>	
	To delete a BGP filter, use the <code>no neighbor {ipv6-address peer-group-name} filter-list as-path-name {in out}</code> command.	

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
	<i>as-path-name</i>	Enter the name of an established AS-PATH access list. If you do not configure the AS-PATH access list, the default is <code>permit</code> (to allow routes). The maximum is 16 characters.
	<i>in</i> <i>out</i>	Enter the keyword <code>in</code> to filter inbound BGP routes. Enter the keyword <code>out</code> to filter outbound BGP routes.
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

neighbor maximum-prefix

Control the number of network prefixes received.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} maximum-prefix maximum [threshold] [warning-only]</code>	
	To return to the default values, use the <code>no neighbor {ipv6-address peer-group-name} maximum-prefix maximum [threshold] [warning-only]</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		 NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>maximum</i>	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
	<i>threshold</i>	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches

	this percentage of the maximum value, the software sends a message. The range is 1 to 100 percent. The default is 75 .	
	warning-only	(OPTIONAL) Enter the keywords <code>warning-only</code> to set the router to send a log message when the maximum value is reached. If you do not set this parameter, the router stops peering when the maximum number of prefixes is reached.
Defaults	<code>threshold = 75</code>	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you configure the <code>neighbor maximum-prefix</code> command and the neighbor receives more prefixes than allowed by the <code>neighbor maximum-prefix</code> command configuration, the neighbor goes down and the <code>show ip bgp summary</code> command displays (<i>prfxd</i>) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the <code>clear ip bgp</code> command for the neighbor or the peer group to which the neighbor belongs or you enter the <code>neighbor shutdown</code> and <code>neighbor no shutdown</code> commands.	
Related Commands	show ip bgp summary – displays the current BGP configuration.	

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} next-hop-self</code> To return to the default setting, use the <code>no neighbor {ipv6-address peer-group-name} next-hop-self</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x::x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
Defaults	Disabled.	

Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If you configure the <code>set ipv6 next-hop</code> command in ROUTE-MAP mode, its configuration takes precedence over the <code>neighbor next-hop-self</code> command.	

neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

Z9500

Syntax	<code>neighbor ipv6-address peer-group peer-group-name</code>	
	To delete a peer from a peer group, use the <code>no neighbor ipv6-address peer-group peer-group-name</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x::x format.
	 NOTE: The :: notation specifies successive hexadecimal fields of zeros.	
	<i>peer-group peer-group-name</i>	Enter the keywords <code>peer-group</code> followed by the name of a configured peer group. The maximum is 16 characters.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	You can assign up to 64 peers to one peer group.	
	When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:	

- [neighbor advertisement-interval](#)
- [neighbor distribute-list](#)
- [neighbor route-map](#)
- [neighbor route-reflector-client](#)
- [neighbor send-community](#)

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown), the peers within the group are also disabled (shutdown).

Related Commands

- [clear ip bgp](#) – resets BGP sessions.
- [neighbor peer-group \(creating group\)](#) – creates a peer group.
- [show ip bgp peer-group](#) – view BGP peers.
- [show ip bgp neighbors](#) show ip bgp neighbors View BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

Z9500

Syntax

`neighbor peer-group-name peer-group`

To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters

peer-group-name Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

When a peer group is created, it is disabled (shut mode).

**Related
Commands**

- [neighbor peer-group \(assigning peers\)](#) – assigns routers to a peer group.
- [neighbor remote-as](#) – assigns an indirectly connected AS to a neighbor or peer group.
- [neighbor shutdown](#) – disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

Z9500

Syntax

```
neighbor peer-group-name peer-group passive
```

To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

Parameters

peer-group-name

Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

**Command
Modes**

ROUTER BGP

**Command
History**

Version

Description

9.2(1.0)

Introduced on the Z9500.

8.2.1.0

Introduced on the E-Series ExaScale.

7.4.1.0

Introduced

**Usage
Information**

After you configure a peer group as passive, you must assign it a subnet using the `neighbor subnet` command.

**Related
Commands**

[neighbor subnet](#) – assigns a subnet to a dynamically-configured BGP neighbor.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} remote-as number
```

To delete a remote AS entry, use the `no neighbor {ipv6-address | peer-group-name} remote-as number` command.

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
	<i>number</i>	Enter a number of the AS. The range is 1 to 65535.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	If the number parameter is the same as the AS number used in the <code>router bgp</code> command, the remote AS entry in the neighbor is considered an internal BGP peer entry.	
	This command creates a peer and the newly created peer is disabled (shutdown).	
Related Commands	router bgp – Enter ROUTER BGP mode and configure routes in an AS.	

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} remove-private-as</code>	
	To return to the default, use the <code>no neighbor {ipv6-address peer-group-name} remove-private-as</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to remove the private AS numbers.
Defaults	Disabled (that is, private AS number are not removed).	

Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Applies to EBGp neighbors only.	
	If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGp neighbor, the private AS numbers are not removed.	
	If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.	
	Private AS numbers are 64512 to 65535.	

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} route-map map-name {in out}</code>	
	To remove the route map, use the <code>no neighbor {ipv6-address peer-group-name} route-map map-name {in out} command</code> .	
Parameters	ipv6-address	Enter the IPv6 address in the x:x:x::x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group-name	Enter the name of the peer group.
	map-name	Enter the name of an established route map. If you do not configure the Route map, the default is <code>deny</code> (to drop all routes).
	in	Enter the keyword <code>in</code> to filter inbound routes.
	out	Enter the keyword <code>out</code> to filter outbound routes.
Defaults	Not configured.	

Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted. If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.	

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Z9500

Syntax	<pre>neighbor {ipv6-address peer-group-name} route-reflector-client</pre> To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the <code>no neighbor {ipv6-address peer-group-name} route-reflector-client</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x:x format.
	 NOTE: The :: notation specifies successive hexadecimal fields of zeros.	
	<i>peer-group-name</i>	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} send-community
```

To disable sending a COMMUNITY attribute, use the `no neighbor {ipv6-address | peer-group-name} send-community` command.

Parameters

ipv6-address

Enter the IPv6 address in the x:x:x::x format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name

Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults

Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version

Description

9.2(1.0)

Introduced on the Z9500.

8.2.1.0

Introduced on the E-Series ExaScale.

7.4.1.0

Introduced

neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

Z9500

Syntax

```
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

Parameters	<i>ipv4-address</i> <i>ipv6-address</i> Enter the IP address of the neighbor for which you want to start storing inbound routing updates. <i>peer-group-name</i> Enter the name of the peer group for which you want to start storing inbound routing updates.														
Defaults	Disabled.														
Command Modes	ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.4.1.0</td><td>Added support for IPv4 multicast and IPv4 unicast address families.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.4.1.0	Added support for IPv4 multicast and IPv4 unicast address families.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Introduced on the S4810.	7.7.1.0	Introduced on the C-Series.	7.4.1.0	Introduced
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.4.1.0	Added support for IPv4 multicast and IPv4 unicast address families.														
8.3.19.0	Introduced on the S4820T.														
7.8.1.0	Introduced on the S4810.														
7.7.1.0	Introduced on the C-Series.														
7.4.1.0	Introduced														
Usage Information	This command enables soft-reconfiguration for the specified BGP neighbor. BGP stores all updates for inbound IPv6 unicast routes the neighbor receives but does not reset the peer-session.  CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.														

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

Z9500

Syntax	<i>neighbor peer-group-name subnet subnet-number mask</i> To remove passive peering, use the <i>no neighbor peer-group-name subnet subnet-number mask</i> command.
Parameters	<i>subnet-number</i> Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the peer group. To allow all addresses, enter 0::0/0.

	mask	Enter a prefix mask in / prefix-length format (/x).
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

neighbor shutdown

Disable a BGP neighbor or peer group.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} shutdown</code> To enable a disabled neighbor or peer group, use the <code>no neighbor {ipv6-address peer-group-name} shutdown</code> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x::x format.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to disable or enable all routers within the peer group.
Defaults	Enabled (that is, BGP neighbors and peer groups are disabled.)	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Peers that are enabled within a peer group are disabled when their peer group is disabled. The <code>neighbor shutdown</code> command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the	

specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp summary` command to confirm its status.

Related Commands

- [show ip bgp summary](#) – displays the current BGP configuration.
- [show ip bgp neighbors](#) – displays the current BGP neighbors.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} timers keepalive  
holdtime
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} timers` command.

Parameters

ipv6-address

Enter the IPv6 address in the x:x:x:x:x format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name

Enter the name of the peer group to set the timers for all routers within the peer group.

keepalive

Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is 1 to 65535. The default is **60 seconds**.

holdtime

Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults

- *keepalive* = **60 seconds**
- *holdtime* = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version

Description

9.2(1.0)

Introduced on the Z9500.

8.2.1.0

Introduced on the E-Series ExaScale.

7.4.1.0

Introduced

Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different *keepalive* and *holdtime* values, negotiate for new values, the resulting values are as follows:

- the lower of the *holdtime* values is the new *holdtime* value, and
- whichever is the lower value; one-third of the new *holdtime* value, or the configured *keepalive* value is the new *keepalive* value.

neighbor update-source

Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

Z9500

Syntax

```
neighbor {ipv6-address | peer-group-name} update-source  
loopback interface
```

To use the closest interface, use the `no neighbor {ipv6-address | peer-group-name} update-source loopback interface` command.

Parameters

ipv6-address

Enter the IPv6 address in the x:x:x:x format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name

Enter the name of the peer group to disable all routers within the peer group.

loopback interface

Enter the keyword `loopback` followed by a number of the loopback interface. The range is 0 to 16383.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version

Description

9.2(1.0)

Introduced on the Z9500.

8.2.1.0

Introduced on the E-Series ExaScale.

7.4.1.0

Introduced

Usage Information

Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Z9500

Syntax	<code>neighbor {ipv6-address peer-group-name} weight weight</code>	
	To remove a weight value, use the <code>no neighbor {ipv6-address peer-group-name} weight weight</code> command.	
Parameters	ipv6-address	Enter the IPv6 address in the x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
	weight	Enter a number as the weight. The range is 0 to 65535. The default is 0 .
Defaults	0	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	In the software's best path selection process, the path with the highest weight value is preferred.	
		NOTE: Reset the neighbor connection (the <code>clear ip bgp *</code> command) to apply the weight to the connection and recompute the best path.

neighbor X:X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

Z9500

Syntax	<code>neighbor x:x:x::x password {7 <encrypt-pass> <clear-pass>}</code>
	To return to the default setting, use the <code>no neighbor x:x:x::x password</code> command.

Parameters	<i>encrypt-pass</i>	Enter the encrypted password.
	<i>clear-pass</i>	Enter the clear text password.
Defaults	Disabled.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced
Usage Information	The TCP session is authentication and hence prevents the data from being compromised.	

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Z9500

Syntax

```
network ipv6-address prefix-length [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters	<i>ipv6-address prefix-length</i>	Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.
		NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	<i>mask</i>	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
	<i>route-map map-name</i>	(OPTIONAL) Enter the keywords <i>route-map</i> followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is <code>deny</code> (to drop all routes).

Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	The software resolves the network address configured by the <code>network</code> command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.	
Related Commands	redistribute – redistributes routes into BGP.	

network backdoor

Specify this IGP route as the preferred route.

Z9500

Syntax	<pre>network ipv6-address prefix-length backdoor</pre> To remove a network, use the <code>no network ipv6-address prefix-length backdoor</code> command.	
Parameters	<i>ipv6-address</i> <i>prefix-length</i>	Enter the IPv6 address in the x:x:x::x format followed by the prefix length in the /x format. The r range is /0 to /128.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	Though the software does not generate a route due to backdoor config, there is an option for injecting/ sourcing a local route in presence of network backdoor config on a learned route.	

redistribute

Redistribute routes into BGP.

Z9500

Syntax	redistribute {connected static} [route-map map-name]	
	To disable redistribution, use the no redistribute [connected static] [route-map map-name] command.	
Parameters		
	connected	Enter the keyword connected to redistribute routes from physically connected interfaces.
	static	Enter the keyword static to redistribute manually configured routes. These routes are treated as incomplete routes.
	route-map map-name	(OPTIONAL) Enter the keywords route-map followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced
Usage Information	If you do not configure the default-metric command in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is "0". To redistribute the default route (0::0/0), configure the neighbor default-originate command.	
Related Commands	neighbor default-originate – injects the default route.	

redistribute ospf

Redistribute OSPFv3 routes into BGP.

Z9500

Syntax	<pre>redistribute ospf process-id [[match external {1 2}] [match internal]] [route-map map-name]</pre>	
	To stop redistribution of OSPF routes, use the <code>no redistribute ospf process-id</code> command.	
Parameters	process-id	Enter the number of the OSPFv3 process. The range is 1 to 65535.
	match external {1 2}	(OPTIONAL) Enter the keywords <code>match external</code> to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
	match internal	(OPTIONAL) Enter the keywords <code>match internal</code> to redistribute OSPFv3 internal routes only.
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: - match ipv6 address - match ipv6 next-hop - match ipv6 route-source - set ipv6 next-hop If you do not configure the route map, the default is <code>deny</code> (to drop all routes).
Defaults	Not configured.	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	When you enter the <code>redistribute ospf process-id</code> command without any other parameters, the software redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.	

router bgp

Enter ROUTER BGP mode to configure and enable BGP.

Z9500

Syntax	<pre>router bgp as-number</pre> To disable BGP, use the <code>no router bgp as-number</code> command.	
Parameters	<i>process-id</i>	Enter the number of the OSPFv3 process. The range is 1 to 65535.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv6 address.

Z9500

Syntax	<pre>show capture bgp-pdu neighbor ipv6-address</pre>	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address (X:X:X:X::X) of a BGP neighbor.
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.5.1.0	Introduced
Related Commands	capture bgp-pdu neighbor – enables capture of an IPv6 BGP neighbor packet. clear ip bgp – specifies a size for the capture buffer.	

show config

View the current ROUTER BGP configuration.

Z9500

Syntax	show config	
Command Modes	ROUTER BGPV6-ADDRESS FAMILY	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.

Example

```
Dell(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown
!
Dell#
```

show ip bgp next-hop

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Z9500

Syntax	show ip bgp next-hop [local-routes]	
Parameters	local-routes	(OPTIONAL) Show next-hop information for local routes.
Command Modes	• EXEC	

- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#show ip bgp next-hop
  Next-hop  Via                      RefCount  Cost  Flaps  Time
Elapsed
  9000::5:2  9000::5:2, Te 2/38  2           0    0    00:23:22
  9000::6:2  9000::6:2, Te 2/38  2           0    0    00:23:22
  9000::7:2  9000::7:2, Te 2/38  2           0    0    00:23:22
  9000::8:2  9000::8:2, Te 2/38  2           0    0    00:23:22
  9000::9:2  9000::9:2, Te 2/38 6000        0    0    00:23:16
  9000::a:2  9000::a:2, Te 2/38  2           0    0    00:23:22
Dell#
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

Z9500

Syntax

```
show ip bgp paths [regexp regular-expression]
```

Parameters

regexp *regular-expression*

Enter a regular expression then use one or a combination of the following characters to match:

- **.** = (period) any single character (including a white space).
- ***** = (asterisk) the sequences in a pattern (0 or more sequences).
- **+** = (plus) the sequences in a pattern (1 or more sequences).
- **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL +v) prior to entering the ? regular expression.
- **[]** = (brackets) a range of single-character patterns.
- **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- **\$** = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

Z9500

Syntax `show ip bgp paths as-path`

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Z9500

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp paths extcommunity

View all unique Extended community information in the BGP database.

Z9500

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp regexp

Allows you to view the subset of BGP routing table matching the regular expressions specified.

Z9500

Syntax `show ip bgp regexp regular-expression [character]`

Parameters

<i>regular-expression</i> [<i>character</i>]	Enter a regular expression then use one or a combination of the following characters to match: • <code>.</code> = (period) any single character (including a white space). • <code>*</code> = (asterisk) the sequences in a pattern (0 or more sequences). • <code>+</code> = (plus) the sequences in a pattern (1 or more sequences). • <code>?</code> = (question mark) sequences in a pattern (either 0 or 1 sequences).  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the <code>?</code> regular expression. • <code>[]</code> = (brackets) a range of single-character patterns. • <code>^</code> = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • <code>\$</code> = (dollar sign) the end of the output string.
---	---

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ipv6 prefix-list

Displays the specified IPv6 prefix list.

Z9500

Syntax	<code>show ipv6 prefix-list detail {<i>prefix-list name</i>} summary</code>	
Parameters	detail	Display a detailed description of the selected IPv6 prefix list.
	<i>prefix-list name</i>	Enter the name of the prefix list.
	 NOTE: There is a 140-character limit for prefix list names.	
	summary	Display a summary of RPF routes.

Command Modes	EXEC
---------------	------

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Related Commands [ipv6 prefix-list](#) — configures an IPv6 prefix-list.

show ip bgp ipv6 unicast

View the current BGP routing table.

Z9500

Syntax	<code>show ip bgp ipv6 unicast [<i>network</i> [<i>network-mask</i>] [<i>longer-prefixes</i>]]</code>
--------	---

Parameters	<i>network</i>	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.								
	<i>network-mask</i>	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.								
	<i>longer-prefixes</i>	(OPTIONAL) Enter the keywords <i>longer-prefixes</i> to view all routes with a common prefix.								
Command Modes	- EXEC - EXEC Privilege									
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.4.1.0</td><td>Introduced</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.2.1.0	Introduced on the E-Series ExaScale.	7.4.1.0	Introduced	
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.2.1.0	Introduced on the E-Series ExaScale.									
7.4.1.0	Introduced									
Usage Information	When you enable the <code>bgp non-deterministic-med</code> command, the <code>show ip bgp</code> command output for a BGP route does not list the INACTIVE reason.									

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

Z9500

Syntax	show ip bgp ipv6 unicast cluster-list [<i>cluster-id</i>]	
Parameters	<i>cluster-id</i>	(OPTIONAL) Enter the cluster id in dotted decimal format.
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp ipv6 unicast community

View information on all routes with Community attributes or view specific BGP community groups.

Z9500

Syntax	<code>show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]</code>	
Parameters	community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
	local-AS	Enter the keywords <code>local-AS</code> to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
	no-advertise	Enter the keywords <code>no-advertise</code> to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
	no-export	Enter the keywords <code>no-export</code> to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Usage Information	To view the total number of COMMUNITY attributes found, use the <code>show ip bgp summary</code> command. The text line above the route table states the number of COMMUNITY attributes found.	

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

Z9500

Syntax	<code>show ip bgp ipv6 unicast community-list <i>community-list-name</i> [exact-match]</code>	
Parameters	<i>community-list-name</i>	Enter the name of a configured IP community list.
	exact-match	(OPTIONAL) Enter exact-match to display only for an exact match of the communities.
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

Z9500

Syntax	<code>show ip bgp ipv6 unicast dampened-paths</code>	
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	7.4.1.0	Introduced

show ip bgp ipv6 unicast detail

Display BGP internal information for IPv6 Unicast address family.

Z9500

Syntax `show ip bgp ipv6 unicast detail`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

Z9500

Syntax `show ip bgp ipv6 unicast extcommunity-list [list name]`

Parameters

<i>list name</i>	Enter the extended community list name you wish to view.
------------------	--

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

Z9500

Syntax `show ip bgp ipv6 unicast filter-list as-path-name`

Parameters

<i>as-path-name</i>	Enter the name of an AS-PATH.
----------------------------	-------------------------------

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

Z9500

Syntax `show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list as-path-name] [regexp regular-expression]`

Parameters

<i>ipv6-address prefix-length</i>	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.
--	--



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

<i>filter-list as-path-name</i>	(OPTIONAL) Enter the keywords <code>filter-list</code> followed by the name of a configured AS-PATH ACL.
--	--

<i>regexp regular-expression</i>	Enter a regular expression then use one or a combination of the following characters to match:
---	--

- . = (period) any single character (including a white space).
- * = (asterisk) the sequences in a pattern (0 or more sequences).

- + = (plus) the sequences in a pattern (1 or more sequences).
- ? = (question mark) sequences in a pattern (either 0 or 1 sequences).



NOTE: You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.

- [] = (brackets) a range of single-character patterns.
- ^ = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- \$ = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Z9500

Syntax

```
show ip bgp ipv6 unicast inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

Z9500

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length
| ip-address] [advertised-routes | dampened-routes | detail |
flap-statistics | routes]
```

Parameters

ipv6-address
prefix-length |
ip-address

Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format. The range is /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros or enter an IP address in dotted decimal format to reset all prefixes from that neighbor.

advertised-routes

(OPTIONAL) Enter the keywords *advertised-routes* to view only the routes the neighbor sent.

dampened-routes

(OPTIONAL) Enter the keywords *dampened-routes* to view information on dampened routes from the BGP neighbor.

detail

(OPTIONAL) Enter the keyword *detail* to view neighbor-specific internal information for the IPv6 address family.

flap-statistics

(OPTIONAL) Enter the keywords *flap-statistics* to view flap statistics on the neighbor's routes.

routes

(OPTIONAL) Enter the keyword *routes* to view only the neighbor's feasible routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands

[show ip bgp](#) – view the current BGP routing table.

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

Z9500

Syntax `show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to view peer-group-specific information for the IPv6 address family.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view status information of the peers in that peer group. The output is the same as that found in <code>show ip bgp summary</code> command

Command Modes

- EXEC
- EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced

Example

```
Dell#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
Dell#
```

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

Z9500

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Example

```
Dell# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory
```

Neighbor State/Pfx	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
1109::33 Active	18508	0	0	0	0	0	never
2222::220 Active	18508	0	0	0	0	0	never
4000::33 Active	18508	0	0	0	0	0	never
4000::60 Active	18508	0	0	0	0	0	never
9000::4:2 Active	18508	0	0	0	0	0	never
9000::5:2 00:16:42	1	35 0	32	0	0	0	
9000::6:2 00:16:39	2	35 0	32	0	0	0	
9000::7:2 00:16:41	3	35 0	32	0	0	0	
9000::8:2 00:16:42	18508	35 0	32	0	0	0	
9000::9:2 00:16:41	18508	44 0	19	0	0	0	
9000::a:2 00:16:43	18508	35 0	32	0	0	0	
9000::b:14 00:13:01	18508	29 0	29	0	0	0	

```
Dell#
```

timers bgp

Allows you to adjust the BGP network timers for all neighbors.

Z9500

Syntax	<code>timers bgp keepalive holdtimer</code>	
	To return to the default values, use the <code>no timers bgp</code> command.	
Parameters	<i>keepalive</i>	Enter the time interval in seconds between which the software sends keepalive messages. The range is 1 to 65535. The default is 60 seconds .
	<i>holdtimer</i>	Enter the time interval in seconds which the software waits since the last keepalive message before declaring a BGP peer dead. The range is 3 to 65535. The default is 180 seconds .
Defaults	• <i>keepalive</i> = 60 seconds • <i>holdtimer</i> = 180 seconds	
Command Modes	ROUTER BGP	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.4.1.0	Introduced
Related Commands	neighbor timers – adjusts BGP timers for a specific peer or peer group.	

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables the multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (AS). MBGP is implemented as per IETF RFC 1858.

show ipv6 mbgproutes

Display the selected IPv6 MBGP route or a summary of all MBGP routes in the table.

Z9500

Syntax	<code>show ipv6 mbgproutes ipv6-address prefix-length summary</code>
--------	--

Parameters

ipv6-address
prefix-length (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

summary Display a summary of RPF routes.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

Content Addressable Memory (CAM)

You can use Content Addressable Memory (CAM) commands to configure the amount of memory allocated to CAM memory partitions.



NOTE: Not all CAM commands are supported on all platforms. Be sure to note the platform when looking for a command.



WARNING: If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance.

CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control lists (ACLs) (when IPv6 is not employed).
- Hash multi-protocol label switching (MPLS) packets based on source and destination IP addresses for link aggregation groups (LAGs).
- Hash based on bidirectional flow for LAGs.
- Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

Important Points to Remember

- All line cards within a single system must have the same CAM profile (including CAM sub-region configurations); this profile must match the system CAM profile (the profile on the primary route processor module [RPM]).
- The system automatically reconfigures the CAM profile on line cards and the secondary RPM to match the system CAM profile by saving the correct profile on the card and then rebooting it.
- The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with `port range` options might require more than one CAM entry.
- After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

cam-acl (Configuration)

Select the default CAM allocation settings or reconfigure a new CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address

validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, OpenFlow, and Policy-based Routing (PBR).

Z9500

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number
ipv4qos number l2qos number l2pt number ipmacacl number ecfmacl
number [vman-qos | vman-dual-qos number] ipv4pbr
number}openflow {4|8} | fcoe number}
```

Parameters	default	Use the default CAM profile settings and set the CAM as follows: • L3 ACL (ipv4acl): 4 • L2 ACL(l2acl): 5 • IPv6 L3 ACL (ipv6acl): 0 • L3 QoS (ipv4qos): 1 • L2 QoS (l2qos): 1 • OpenFlow: 0 (disabled)
	l2acl number ipv4acl number ipv6acl number, ipv4qos number l2qos number l2pt number ipmacacl number ecfmacl number [vman- qos vman- dual-qos number] ipv4pbr numberopenflo w {4 8} fcoe number	Allocate space to each CAM region. Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The range for ipv4acl is from 1 to 4. The ipv6acl range must be a factor of 2. Enter 4 or 8 for the number of OpenFlow FP blocks. • 4: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality) • 8: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality) The fcoe range is 0–6 groups. Each group has 128 entries; the value given must be an even number. This information is stored in the NVRAM and is effective after rebooting the switch.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for fcoe.
9.1(0.0)	Added support for OpenFlow.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.2	Clarified block information for the S4810.
8.3.10.0	Introduced on the S4810.
8.3.1.0	Added the keywords <code>ecfmac1</code> , <code>vman-qos</code> , and <code>vman-dual-qos</code> .
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

Save the new CAM settings to the startup-config (`write mem` or `copy run start`) then reload the system for the new settings to take effect.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated. The `ipv4acl` profile range is from 1 to 4.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

If allocation values are not entered for the CAM regions, the value is 0.

If you enable BMP 3.0, to perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, use the command `reload conditional nvram-cfg-change`.

cam-acl-egress

Allocate CAM for egress ACLs.

Z9500

Syntax

```
cam-acl-egress default | l2acl number ipv4acl number ipv6acl
number}
```

Parameters

default	Reset egress CAM ACL entries to default settings.
l2acl number	Allocate space to each CAM region.
ipv4acl number	
ipv6acl number	

Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The range for ipv4acl is from 1 to 4. The ipv6acl range must be a factor of 2.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Z9500

Syntax `cam-optimization [qos]`

Parameters **qos** Optimize CAM usage for QoS.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.

	Version	Description
	7.8.1.0	Introduced on the C-Series.
Usage Information	When you enable this command, if a Policy Map containing classification rules (ACL and/or dscp/ ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy is written (only one FP entry is used).  NOTE: An ACL itself may still require more than a single FP entry, regardless of the number of interfaces. For more information, refer to the "IP Access Control Lists", "Prefix Lists", and "Route-map" sections in the <i>Dell Networking OS Configuration Guide</i>.	

show cam-acl

Display the details of the CAM profiles on the chassis and all line cards.

Z9500

Syntax	show cam-acl
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series.

Usage Information	The display reflects the settings implemented with the <code>cam-acl</code> command.
--------------------------	--

Example	<pre> Dell#show cam-acl -- Chassis Cam ACL -- Current Settings(in block sizes) 1 block = 256 entries L2Acl : 2 Ipv4Acl : 2 Ipv6Acl : 4 Ipv4Qos : 2 L2Qos : 2 L2PT : 1 </pre>
----------------	--

```

IpMacAcl      :      0
VmanQos       :      0
EcfmAcl       :      0
Openflow      :      0

-- linecard 0 --
      Current Settings(in block sizes)
      1 block = 256 entries
L2Acl         :      2
Ipv4Acl       :      2
Ipv6Acl       :      4
Ipv4Qos       :      2
L2Qos         :      2
L2PT          :      1
IpMacAcl      :      0
VmanQos       :      0
EcfmAcl       :      0
Openflow      :      0

-- linecard 1 --
      Current Settings(in block sizes)
      1 block = 256 entries
L2Acl         :      2
Ipv4Acl       :      2
Ipv6Acl       :      4
Ipv4Qos       :      2
L2Qos         :      2
L2PT          :      1
IpMacAcl      :      0
VmanQos       :      0
EcfmAcl       :      0
Openflow      :      0

-- linecard 2 --
      Current Settings(in block sizes)
      1 block = 256 entries
L2Acl         :      2
Ipv4Acl       :      2
Ipv6Acl       :      4
Ipv4Qos       :      2
L2Qos         :      2
L2PT          :      1
IpMacAcl      :      0
VmanQos       :      0
EcfmAcl       :      0
Openflow      :      0

Dell#

```

test cam-usage

Verify the CAM space that is available for IPv4 and IPv6 CAM profiles, and particularly to verify if enough CAM space is available for the IPv6 ACLs you use in a policy map.

Z9500

Syntax

```
test cam-usage service-policy input policy-map-name linecard
{number portset {port-pipe-number} | all}
```

Parameters	input <i>policy-map-name</i>	Enter the name of the policy map to verify. Maximum is 32 characters.												
	linecard <i>number</i> portset <i>port-pipe-number</i>	Enter a line card and port-pipe number to check CAM usage on specified ports. The range of valid port-pipe numbers is 0 to 3. Enter <code>linecard all</code> to verify the CAM space available for all ports on the switch.												
Defaults	none													
Command Modes	EXEC Privilege													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.8.1.0	Introduced.													
Usage Information	This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs. QoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces. The following describes the <code>test cam-usage</code> command shown in the following example. <table><tr><th>Term</th><th>Explanation</th></tr><tr><td>Linecard</td><td>Lists the line cards that are checked. Entering <code>all</code> displays the status for line cards in the chassis.</td></tr><tr><td>Portpipe</td><td>Lists the port pipes (port sets) that are checked. Entering <code>all</code> displays the status for all line cards and port pipes in the chassis.</td></tr><tr><td>CAM Partition</td><td>Shows the CAM profile of the CAM.</td></tr><tr><td>Available CAM</td><td>Identifies the amount of CAM space remaining for that profile.</td></tr></table>		Term	Explanation	Linecard	Lists the line cards that are checked. Entering <code>all</code> displays the status for line cards in the chassis.	Portpipe	Lists the port pipes (port sets) that are checked. Entering <code>all</code> displays the status for all line cards and port pipes in the chassis.	CAM Partition	Shows the CAM profile of the CAM.	Available CAM	Identifies the amount of CAM space remaining for that profile.		
Term	Explanation													
Linecard	Lists the line cards that are checked. Entering <code>all</code> displays the status for line cards in the chassis.													
Portpipe	Lists the port pipes (port sets) that are checked. Entering <code>all</code> displays the status for all line cards and port pipes in the chassis.													
CAM Partition	Shows the CAM profile of the CAM.													
Available CAM	Identifies the amount of CAM space remaining for that profile.													

Term	Explanation
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM.

Example

```
Dell# test cam-usage service-policy input pcam linecard all
linecard | Portpipe | CAM Partition | Available CAM |
Estimated CAM per Port | Status
```


	0	0	IPv4Flow	408
		1	Allowed (408)	
	0	1	IPv4Flow	408
		1	Allowed (408)	
	0	2	IPv4Flow	408
		1	Allowed (408)	
	1	0	IPv4Flow	408
		1	Allowed (408)	
	1	1	IPv4Flow	408
		1	Allowed (408)	
	1	2	IPv4Flow	408
		1	Allowed (408)	
	1	3	IPv4Flow	408
		1	Allowed (408)	
	2	0	IPv4Flow	408
		1	Allowed (408)	
	2	1	IPv4Flow	408
		1	Allowed (408)	
	2	2	IPv4Flow	408
		1	Allowed (408)	
	2	3	IPv4Flow	408
		1	Allowed (408)	

Control Plane Policing (CoPP)

Control plane policing (CoPP) uses access control list (ACL) rules and quality of service (QoS) policies to create filters for a system’s control plane. The CoPP filters prevent traffic that is not identified as legitimate from reaching the control plane, and rate-limit traffic to an acceptable level.

On the Z9500 switch, the control plane has 24 queues (0 to 23) divided into groups of eight queues for the Route Processor, Control Processor, and line-card CPUs as follows:

- Queues 0 to 7 process packets destined to the Control Processor CPU .
- Queues 8 to 15 process packets destined to the Route Processor CPU.
- Queues 16 to 23 process packets destined to the line card CPU.

clear control-traffic protocol

Clear all per-protocol counters of rate-limited control-plane traffic.

Z9500

Syntax	<code>clear control-traffic protocol [cp-switch linecard slot-id portset port-pipe] counters</code>	
Parameters	cp-switch	Enter the keyword <code>cp-switch</code> to display counters for rate-limited traffic on the central switch (aggregated CoPP).
	linecard slot-id portset port-pipe	Enter the slot ID and port pipe to display counters for rate-limited traffic on a specified Z9500 line card and port set. The range of Z9500 slot IDs is from 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.
Defaults	Clear per-protocol rate-limiting counters for all control-plane and port-set (port-pipe) traffic.	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information

There are three line cards (0-2) with fixed ports on the Z9500. Line card 0 uses three sets of ports (port pipes): 0 to 2; line cards 1 and 2 use four sets of ports: 0 to 3.

- On line card 0, port set 0 consists of ports 0–44; port set 1 consists of ports 48–92; port set 2 consists of ports 96–140.
- On line cards 1 and 2, port set 0 consists of ports 0–44; port set 1 consists of ports 48–92; port set 2 consists of ports 96–140; port set 3 consists of ports 144–188.

To display the per-protocol counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the `show control-traffic protocol` command.

Example

```
Dell#clear control-traffic protocol cp-switch counters
Dell#
```

clear control-traffic queue

Clear per-queue counters of rate-limited control-plane traffic.

Z9500

Syntax

```
clear control-traffic queue {all | queue-number} counters
```

Parameters

- | | |
|----------------------------|--|
| all | Enter the keyword <code>all</code> to clear counters for rate-limited traffic on all CPU queues, including Route Processor, Control Processor, and line-card CPUs. |
| <i>queue-number</i> | <p>Enter the queue number to clear counters for rate-limited traffic on a specified CPU queue. The range of queue-number values is from 0 to 23. The twenty-four control-plane queues are divided into groups of eight queues for the Route Processor, Control Processor, and line-card CPUs as follows:</p> <ul style="list-style-type: none"> • Queues 0 to 7 process packets destined to the Control Processor CPU. • Queues 8 to 15 process packets destined to the Route Processor CPU. |

- Queues 16 to 23 process packets destined to the line card CPU.

Defaults	Clear per-queue rate-limiting counters for all control-plane and port traffic.										
Command Modes	EXEC Privilege										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.8.0	Introduced on the S4810.										
Usage Information	To display the per-queue counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the <code>show control-traffic queue</code> command.										
Example	<pre>Dell#clear control-traffic queue 2 counters Dell#</pre>										

control-plane-cpuqos

To manage control-plane traffic, enter control-plane mode and configure the switch.

Z9500

Syntax	<code>control-plane-cpuqos</code>
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

service-policy rate-limit-cpu-queues cpu-qos

Apply a QoS input policy-map that rate-limits traffic on control-plane queues.

Z9500

Syntax	<code>service-policy rate-limit-cpu-queues <i>policy-name</i> cpu-qos</code>
Parameters	<i>policy-name</i> Enter the service-policy name, using a string up to 32 characters.
Defaults	Not configured.
Command Modes	CONTROL-PLANE-CPUQOS
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information	Create a policy-map by associating a queue number with the qos-policy. Create QoS policies prior to enabling this command. When you apply a QoS input policy-map for rate-limiting control-plane traffic (CoPP), you must enter the keyword <code>cpu-qos</code>.
Related Commands	qos-policy-input cpu-qos — creates a QoS input-policy map for CoPP.

[policy-map-input cpu-qos](#) — creates an input-policy map for CoPP.

service-policy rate-limit-protocols cpu-qos

Apply a QoS input policy-map that rate-limits protocol traffic on the control plane.

Z9500

Syntax	service-policy rate-limit-protocols <i>policy-name</i> cpu-qos											
Parameters	<i>policy-name</i>	Enter the service-policy name, using a string up to 32 characters.										
Defaults	Not configured.											
Command Modes	CONTROL-PLANE-CPUQOS											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Introduced on the S4810.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.19.0	Introduced on the S4820T.											
8.3.11.1	Introduced on the Z9000.											
8.3.8.0	Introduced on the S4810.											
Usage Information	This command applies the service-policy based on the type of protocol defined in the ACL rules. Create ACL and QoS policies prior to enabling this command. When you apply a QoS input policy-map for rate-limiting control-plane traffic (CoPP), you must enter the keyword <code>cpu-qos</code>. If you configure rate-limiting of control protocols on a per-protocol basis and if you modify the rate using the <code>rate-police</code> command in QOS-POLICY-IN mode while traffic is being passed, packet drops for the specified protocols may occur if you configure a rate higher than the default rate for a protocol.											
Related Commands	ip access-list extended cpu-qos — creates an extended IP ACL for CoPP. mac access-list extended cpu-qos — creates an extended MAC ACL for CoPP.											

[class-map cpu-qos](#) — creates a QoS class map for CoPP.

[qos-policy-input cpu-qos](#) — creates a QoS input-policy map for CoPP.

[policy-map-input cpu-qos](#) — creates an input-policy map for CoPP.

show control-traffic protocol

Display per-protocol counters of rate-limited control-plane traffic.

Z9500

Syntax	show control-traffic protocol [cp-switch linecard slot-id portset port-pipe] counters					
Parameters	cp-switch	Enter the keyword cp-switch to display counters for rate-limited traffic on the central switch (aggregated CoPP).				
	linecard slot-id portset port-pipe	Enter the slot ID and port pipe to display counters for rate-limited traffic on a specified Z9500 line card and port set. The range of Z9500 slot IDs is from 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.				
Defaults	None					
Command Modes	EXEC Privilege					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					
Usage Information	There are three line cards (0-2) with fixed ports on the Z9500. Line card 0 uses three sets of ports (port pipes): 0 to 2; line cards 1 and 2 use four sets of ports: 0 to 3. In the show control-traffic protocol output, RxBytes displays the number of bytes of control-plane traffic received on which protocol-based rate limiting is applied. TxBytes displays the number of bytes transmitted to a control-plane CPU after protocol-based rate limiting is applied. Drops displays the number of bytes of control-plane traffic that have been dropped as a result of protocol-based rate limiting.					

The number of RxBytes is calculated as: $\text{Drops} / \langle \text{packet-size} \rangle + \text{TxBytes} / \langle \text{packet-size} + 4 \text{ bytes} \rangle = \text{RxBytes (total packets received)}$

To clear the per-protocol counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the `clear control-traffic protocol` command.

Example

```
Dell#show control-traffic protocol linecard 2 portset 0
counters
  Protocol
  TxBytes      Drops      RxBytes
  -----
  -----
  STP          14956278172
  403036      14955875136
  LLDP         15029657016
  559096      15029097920
  PVST         0
  0            0
  LACP         15122824104
  556648      15122267456
  GVRP         14988129080
  551480      14987577600
  ARP RESP/ARP REQ 29604578172
  3559868      29601018304
  802.1x       0
  0            0
  FEFD         0
  0            0
  FRRP         0
  0            0
  ECFM         0
  0            0
  L2PT         0
  0            0
  ISIS         0
  0            0
  BFD          0
  0            0
  BGP          0
  0            0
  v6 BGP       0
  0            0
  OSPF         0
  0            0
  v6 OSPF      0
  0            0
  RIP          0
  0            0
  VRRP         0
  0            0
  v6 VRRP      0
  0            0
  IGMP         0
  0            0
  PIM          0
  0            0
  NTP          0
  0            0
  MULTICAST CATCH ALL 0
  0            0
```

```

v6 MULTICAST CATCH ALL      0
0                             0
DHCP RELAY/DHCP             0
0                             0
v6 ICMP NA/v6 ICMP RA      0
0                             0
v6 ICMP NS/v6 ICMP RS      0
0                             0
v6 ICMP/ICMP                0
0                             0
MLD                          0
0                             0
MSDP                         0
0                             0
FTP/TELNET/SSH/
L3 LOCAL TERMINATED        0
0                             0
L3 UNKNOWN/UNRESOLVED ARP  0
0                             0
iSCSI                       0
0                             0
FCoE                        0
0                             0
SFLOW                       0
0                             0
VLT CTRL/VLT IPM PDU       0
0                             0
HYPERPULL                   0
0                             0
OPENFLOW                    0
0                             0
L2 DST HIT/BROADCAST       0
0                             0
VLT TTL1/TRACEFLOW/TTL0/
STATION MOVE/TTL1/IP OPTION/
L3 MTU FAIL/SOURCE MISS   0
0                             0

```

show control-traffic queue

Display per-queue counters of rate-limited control-plane traffic.

Z9500

Syntax	show control-traffic queue {all queue-id <i>queue-number</i> } counters	
Parameters	all	Enter the keyword <i>all</i> to display counters for rate-limited traffic on all CPU queues, including Route Processor, Control Processor, and line-card CPUs.
	queue-id <i>queue-number</i>	Enter the queue number to display counters for rate-limited traffic on a specified CPU queue. The range of queue-number values is from 0 to 23. The twenty-four control-plane queues are divided into groups of eight queues for the

Route Processor, Control Processor, and line-card CPUs as follows:

- Queues 0 to 7 process packets destined to the Control Processor CPU .
- Queues 8 to 15 process packets destined to the Route Processor CPU.
- Queues 16 to 23 process packets destined to the line card CPU.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information In the `show` output, Rx Bytes displays the number of bytes of control-plane traffic received, on which queue-based rate limiting is applied. Tx Counters displays the number of bytes transmitted to a control-plane CPU after queue-based rate limiting is applied. Drop Counters displays the number of bytes of control-plane traffic that have been dropped as a result of queue-based rate limiting.

To clear the per-queue counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the `clear control-traffic queue` command.

Example

```
Dell#show control-traffic queue queue-id 0 counters
Queue      Rx Counter    Tx Counter    Drop counter
-----
Q0          5000          5000          0
Dell#
```

show cpu-queue rate

Display the rates for each control-plane queue.

Z9500

Syntax	<code>show cpu-queue rate [all queue-id <i>queue-number</i> range <i>from_queue to_queue</i>]</code>	
Parameters	all	Display the rate for all control-plane queues (CPU queues 0–23).
	queue-id queue-number	Display the rate for a specified control-plane queue. The range of CPU queue values is from 0 to 23.
	range from_queue to_queue	Display the rate for a range of control-plane queues. The range of CPU queue values is from 0 to 23. Separate the <i>from_queue</i> value from the <i>to_queue</i> value with a space; for example, <code>show cpu-queue rate range 8 15</code> .
Defaults	Not configured.	
Command Modes	EXEC Privilege	
Usage Information	This command applies the service-policy based on the type of protocol defined in the ACL rules. Create ACL and QoS policies prior to enabling this command.	

Example	<pre>Dell# show cpu-queue rate all</pre>		
	Service-Queue	Rate (kbps)	Burst (kb)
	-----	-----	-----
	Q0	1000	1000
	Q1	400	1000
	Q2	1800	1000
	Q3	1800	1000
	Q4	2800	5000
	Q5	300	2000
	Q6	300	2000
	Q7	3200	3000
	Q8	400	1000
	Q9	400	1000
	Q10	1800	1000
	Q11	1800	1000
	Q12	2000	6000
	Q13	5200	3000
	Q14	1850	3000
	Q15	12450	4000
	Q16	1	100
	Q17	1	100
	Q18	1	100
	Q19	1	100
	Q20	600	1000
	Q21	7000	7000

Q22	800	1000
Q23	5000	5000

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

show ip protocol-queue-mapping

Display the Z9500 CPU queue mapping for IPv4 protocols.

Z9500

Syntax `show ip protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Usage Information The `show` output displays information on CPU traffic flows for IPv4 protocols, including the ingress queue at which the traffic is queued and the CPU to which protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ip protocol-queue-mapping
```

Protocol Rate (kbps)	Src-Port	Dst-Port	TcpFlag	Queue	EgPort
-----	-----	-----	-----	-----	-----
TCP (BGP) RP	any/179 2500	179/any	—	Q15	
UDP (DHCP) CP	67/68 1200	68/67	—	Q7	
UDP (DHCP-R) CP	67 1200	67	—	Q7	
TCP (FTP) CP	any 400	21	—	Q4	
ICMP CP	any 300	any	—	Q6	
IGMP RP	any 300	any	—	Q14	
TCP (MSDP) RP	any/639 100	639/any	—	Q14	
UDP (NTP) CP	any 200	123	—	Q4	
OSPF RP	any 2500	any	—	Q15	
PIM RP	any 300	any	—	Q14	
UDP (RIP) RP	any 200	520	—	Q15	
TCP (SSH) CP	any 400	22	—	Q4	
TCP (TELNET) CP	any 400	23	—	Q4	
VRRP RP	any 400	any	—	Q15	

show ipv6 protocol-queue-mapping

Display the Z9500 CPU queue mapping for IPv6 protocols.

Z9500

Syntax `show ipv6 protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Usage Information The show output displays information CPU traffic flows for supported IPv6 protocols, including the ingress queue at which the traffic is queued and the CPU to which protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ipv6 protocol-queue-mapping
```

Protocol Rate (kbps)	Src-Port	Dst-Port	TcpFlag	Queue	EgPort
-----	-----	-----	-----	-----	-----
TCP (BGP) RP	any/179 2500	179/any	—	Q15	
ICMPV6 NA RP	any 600	any	—	Q3/Q11	CP/
ICMPV6 RA RP	any 600	any	—	Q3/Q11	CP/
ICMPV6 NS RP	any 600	any	—	Q2/Q10	CP/
ICMPV6 RS RP	any 600	any	—	Q2/Q10	CP/
ICMPV6 CP	any 300	any	—	Q5	
VRRPV6 RP	any 400	any	—	Q15	
OSPFV3 RP	any 2500	any	—	Q15	

show mac protocol-queue-mapping

Display the Z9500 CPU queue mapping for MAC protocols.

Z9500

Syntax `show mac protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show mac protocol-queue-mapping

  Protocol      Destination Mac      EtherType      Queue
  EgPort      Rate
              (kbps)
  -----
  ARP          any          0x0806      Q2/Q10/Q3/
  Q11  CP/RP      600
  FRRP          01:01:e8:00:00:10/11  any
  Q22          LP          300
  LACP          01:80:c2:00:00:02      0x8809
  Q15          RP          500
  LLDP          any          0x88cc
  Q7           CP          500
  GVRP          01:80:c2:00:00:21      any
  Q14          RP          200
  STP          01:80:c2:00:00:00      any
  Q15          RP          150
  ISIS          01:80:c2:00:00:14/15  any
  Q15          RP          500
              09:00:2b:00:00:04/05  any
  Q15          RP          500
```

show protocol-queue-mapping

Display the Z9500 protocol-queue mapping for each configured protocol.

Z9500

Syntax	<code>show protocol-queue-mapping [queue-id queue-number]</code>
Parameters	queue-id (Optional) Display the protocol-queue mapping for a specified control-plane queue. The range of CPU queue numbers is from 0 to 23. queue-number
Defaults	Not configured.
Command Modes	EXEC Privilege
Usage Information	The <code>show</code> output displays information on CPU traffic flows for all protocols, including the ingress queue at which the traffic is queued and the CPU to which

protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell# show protocol-queue-mapping
```

CommitBurst	PeakBurst	Queue	EgPort	CommitRate	Peak Rate
Protocol (kbps)	(kb)	(kb)		(kbps)	
STP		Q15	RP	150	
150	1000	1000			
LLDP		Q7	CP	500	
500	1000	1000			
PVST		Q14	RP	200	
200	1000	1000			
LACP		Q15	RP	500	
500	1000	1000			
ARP		Q2/Q10/Q3/Q11	CP/RP	600	
600	1000	1000			
GVRP		Q14	RP	200	
200	1000	1000			
FRRP		Q22	LP	300	
300	1000	1000			
ECFM		Q15	RP	150	
150	1000	1000			
ISIS		Q15	RP	500	
500	3000	3000			
L2PT		Q15	RP	150	
150	1000	1000			
v6 BGP		Q15	RP	2500	
2500	2000	2000			
v6 OSPF		Q15	RP	2500	
2500	2000	2000			
v6 VRRP		Q15	RP	400	
400	2000	2000			
MLD		Q14	RP	150	
150	500	500			
v6 MULTICAST		Q9	RP	100	
100	500	500			
CATCH ALL					
v6 ICMP NA		Q3/Q11	CP/RP	600	
600	1000	1000			
v6 ICMP RA		Q3/Q11	CP/RP	600	
600	1000	1000			

v6 ICMP NS		Q2/Q10	CP/RP	600
600	1000	1000		
v6 ICMP RS		Q2/Q10	CP/RP	600
600	1000	1000		
v6 ICMP		Q5	CP	300
300	2000	2000		
BGP		Q15	RP	2500
2500	2000	2000		
OSPF		Q15	RP	2500
2500	2000	2000		
RIP		Q15	RP	200
200	1000	1000		
VRRP		Q15	RP	400
400	2000	2000		
ICMP		Q6	CP	300
300	2000	2000		
IGMP		Q14	RP	300
300	2000	2000		
PIM		Q14	RP	300
300	2000	2000		
MSDP		Q14	RP	100
100	2000	2000		
BFD		Q13/Q21	RP/LP	7000
7000	3000	3000		
802.1x		Q7	CP	150
150	1000	1000		
iSCSI		Q9	RP	100
100	500	500		
DHCP RELAY		Q7	CP	1200
1200	2000	2000		
DHCP		Q7	CP	1200
1200	2000	2000		
NTP		Q4	CP	200
200	2000	2000		
FTP		Q4	CP	400
400	3000	3000		
TELNET		Q4	CP	400
400	2000	2000		
SSH		Q4	CP	400
400	2000	2000		
VLT CTRL		Q12	RP	2000
2000	3000	3000		
VLT IPM PDU		Q4/Q12	CP/RP	500
500	3000	3000		
VLT TTL1		Q0	CP	100
100	500	500		
HYPERPULL		Q22	LP	500
500	1000	1000		
OPENFLOW		Q14	RP	300
300	1000	1000		
FEFD		Q7	CP	150
150	1000	1000		
TRACEFLOW		Q20	LP	200
200	500	500		
FCoE		Q14	RP	300
300	2000	2000		
SFLOW		Q23	LP	5000
5000	3000	3000		
L3 LOCAL TERMINATED		Q4	CP	400
400	5000	5000		
L3 UNKNOWN/		Q8	RP	200
200	3000	3000		
UNRESOLVED ARP				
L2 DST HIT/		Q0/Q8	CP/RP	200

200	500	500		
BROADCAST				
MULTICAST CATCH ALL	Q9		RP	200
200	500	500		
ACL LOGGING	Q20		LP	200
200	1000	1000		
L3 HEADER ERROR/TTL0	Q0		CP	200
200	500	500		
IP OPTION/TTL1	Q0		CP	100
100	500	500		
VLAN L3 MTU FAIL	Q1		CP	200
200	500	500		
Physical L3 MTU FAIL	Q1		CP	200
200	500	500		
ICMP REDIRECT	Q1		CP	200
200	500	500		
SOURCE MISS	Q20		LP	200
200	500	500		
STATION MOVE	Q20		LP	200
200	500	500		

Debugging and Diagnostics

Use the debugging and diagnostics commands described in this chapter to troubleshoot switch operation.

This chapter contains the following sections:

- [Offline Diagnostic Commands](#)
- [Buffer Tuning Commands](#)
- [Hardware Commands](#)

Offline Diagnostic Commands

Use the offline diagnostics test suite to isolate faults and debug switch hardware. While tests are running, the system results are saved as a text file in the flash directory: `TestReport-N.txt`, where *N* is 0,1, or 2 for the line-card processor (LP) and 0 for the Control processor (CP) and Route Processor (RP). To display the system results in this text file, use the `show file` command.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected to via a stacking link.
- Diagnostic results are printed to the screen. The Dell Networking OS does not write them to memory.
- Diagnostics only test connectivity, not the entire data path.

diag

Run offline diagnostics on all CPUs or on a specified CPU in the switch.

Z9500

Syntax	<code>diag {all {{cp rp linecard} unit-id} [alllevels level0 level1 level2] [interactive] [testname name] [terminate]}</code>	
Parameters	all	Enter the keyword <code>all</code> to run offline diagnostic tests on all Z9500 CPUs, including the Control Processor, Route Processor, and line cards.
	cp unit-id	Enter the <code>cp unit-id</code> parameters to run offline diagnostic tests only on the Control Processor CPU. The Control Processor CPU ID is 0.

rp <i>unit-id</i>	Enter the keyword <code>rp unit-id</code> parameters to run offline diagnostic tests only on the Route Processor CPU. The Route Processor CPU ID is 0.
linecard <i>unit-id</i>	Enter the <code>linecard unit-id</code> parameters to run offline diagnostic tests only on a specified line card. The range of line-card CPU IDs is from 0 to 2. Each line-card CPU processes packets on the corresponding Z9500 line card; for example, line-card CPU 1 processes packets on line card 1.
alllevels	Enter the keyword <code>alllevels</code> to run the complete set of offline diagnostic tests.
level0	Enter the keyword <code>level0</code> to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword <code>level1</code> to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, ports are shut down automatically.
level2	Enter the keyword <code>level2</code> to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.
interactive	Enter the keyword <code>interactive</code> to run offline diagnostics in interactive mode.
testname <i>name</i>	Enter the <code>testname name</code> parameters to run a specified offline diagnostic test. Enclose the test-case name in double quotes (" "). For example: <code>diag level1 testname "first"</code> .
terminate	Enter the keyword <code>terminate</code> to stop the offline diagnostic tests that are running.

Defaults All offline diagnostic tests are run on all Z9500 CPUs (Control Processor, Route Processor, and line cards).

Command Modes EXEC Privilege

Usage Information

Before you use this command to run diagnostic test, make sure the switch is offline (`offline system` command).

You are prompted to reboot when the off-line diagnostics complete.

Use the `show diag` command to view a summary of diagnostic information presented for each Z9500 CPU.

At the end of offline diagnostic tests, a test report is generated. The filename of the report is `TestReport-{CP/LP/RP}-N.txt`, where `{CP/LP/RP}-N` identifies the CPU and CPU ID on which the diagnostics were run: Route Processor 0, Control Processor 0 or a line-card CPU `{0-2}`. The report is stored at `flash://` and `ramdisk:/diagnostic`. To view the test report, use the `show file flash://filename` command. A sample *filename* is `TestReport-LP-2`.

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the <code>verbose</code> option.
7.7.1.0	Introduced on the S-Series.

Related Commands

[offline stack-unit](#) — bring a switch offline to run diagnostic tests.

[online stack-unit](#) — reload the system after running offline diagnostic tests.

offline system

Place the switch in the offline state in order to run diagnostic tests.

Z9500

Syntax `offline system`

Defaults `none`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added a warning message to the off-line diagnostic.
7.7.1.0	Introduced on the S-Series.

Usage Information

To run diagnostic tests on an offline switch, use the `diag` command.

The system reboots when offline diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline system` command is implemented.

Warning - Diagnostic execution will cause system to reboot after completion of diags.

Proceed with Offline-Diags [confirm yes/no]:y

Related Commands

[diag](#) — run diagnostic tests on an offline switch.

[online stack-unit](#) — reload the system after running offline diagnostic tests.

online system

Reload a switch after running offline diagnostic tests.

Z9500

Syntax `online system`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4810.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.7.1.0	Introduced on the S-Series.
Usage Information	This command is used to manually reset or reboot the system when diagnostics complete.	
Related Commands	diag — run diagnostic tests on an offline switch. offline stack-unit — bring the system offline to run diagnostic tests.	

show diag

Display results of offline diagnostic tests on a switch.

Z9500

Syntax	<code>show diag {all {{cp rp linecard} unit-id} [summary detail]}</code>	
Parameters	all	Enter the keyword <code>all</code> to display the results of offline diagnostic tests on all Z9500 CPUs, including the Control Processor, Route Processor, and line cards.
	cp <i>unit-id</i>	Enter the <code>cp unit-id</code> parameters to display the results only of the offline diagnostic tests run on the Control Processor CPU. The Control Processor CPU ID is 0.
	rp <i>unit-id</i>	Enter the <code>rp unit-id</code> parameters to display the results only of the offline diagnostic test run on the Route Processor CPU. The Route Processor CPU ID is 0.
	linecard <i>unit-id</i>	Enter the <code>linecard unit-id</code> parameters to display the results only of the offline diagnostic test run on a specified line card. The range of line-card CPU IDs is from 0 to 2. Each line-card CPU processes packets on the corresponding Z9500 line card; for example, line-card CPU 1 processes packets on line card 1.
	summary	Enter the keyword <code>summary</code> to display a summary of the offline diagnostic test results.
	detail	Enter the keyword <code>detail</code> to display detailed information about the offline diagnostic test results.
Defaults	A summary of the results of offline diagnostic tests run on all Z9500 CPUs (Control Processor, Route Processor, and line cards) is displayed.	

Command Modes	EXEC Privilege														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.1.0</td><td>Introduced the <code>verbose</code> option.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Introduced the <code>verbose</code> option.	7.7.1.0	Introduced on the S-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.3.1.0	Introduced the <code>verbose</code> option.														
7.7.1.0	Introduced on the S-Series.														
Usage Information	Use the <code>show diag</code> command to view a summary of diagnostic information presented for each Z9500 CPU. CPU diagnostic results are presented in the following order: Control Processor (CP), line-card processor 0 (LP0), line-card processor 1 (LP1), line-card processor 2 (LP2), and Route Processor (RP).														
Example: While offline diagnostics are running on a line card	<pre> Dell# show diag linecard 0 detail Diag status of linecard member 0: ----- linecard is currently offline. linecard level0 diag issued at Wed Jan 08, 2014 04:39:58 AM. Current diag status : Card diags are in progress. Last notification received at Wed Jan 08, 2014 04:40:05 AM Last notification message : Testing ... rtcTest Dell# show diag linecard 0 summary Diag status of linecard member 0: ----- linecard is currently offline. linecard level0 diag issued at Wed Jan 08, 2014 04:39:57 AM. Current diag status : Card diags are in progress. Last notification received at Wed Jan 08, 2014 04:40:04 AM Last notification message : Testing ... rtcTest </pre>														
Example: After offline diagnostics are run on a line card	<pre> Dell# show diag linecard 0 summary Diag status of linecard member 0: ----- linecard is currently offline. linecard level0 diag issued at Wed Jan 08, 2014 04:39:58 AM. Current diag status : Card diags are done. Duration of execution (Total) : 0 min 31 sec. </pre>														

Diagnostic test results located: flash:/TestReport-
LP-0.txt
Last notification received at Wed Jan 08, 2014 04:40:29 AM
Last notification message : Level0 diag done.

```
DELL  DIAGNOSTIC  [0]

PPID                -- NA
PPID Rev            -- NA
Service Tag         -- NA
Part Number         -- NA
Part Number Revision -- NA
SW Version          -- 9-2(1-509)
```

Available free memory: 2,635,960,320 bytes

```
----- Group Test Statistics -----
Total      : 11
Passed     : 9
Failed     : 2
Elapsed time : 00H:00M:18S
Stop reason : after completion
----- Failed tests (level, times) -----
                i2cTest (0, 1)
                qsfpOpticsTest (0, 1)
```

Dell# show diag linecard 0 detail
Diag status of linecard member 0:

```
linecard is currently offline.
linecard level0 diag issued at Wed Jan 08, 2014 04:39:58
AM.
Current diag status      : Card diags are done.
Duration of execution (Total) : 0 min 31 sec.
Diagnostic test results located: flash:/TestReport-
LP-0.txt
Last notification received at Wed Jan 08, 2014 04:40:29 AM
Last notification message : Level0 diag done.
```

```
DELL  DIAGNOSTIC  [0]

PPID                -- NA
PPID Rev            -- NA
Service Tag         -- NA
Part Number         -- NA
Part Number Revision -- NA
SW Version          -- 9-2(1-509)
```

Available free memory: 2,635,960,320 bytes

LEVEL 0 DIAGNOSTIC

```

eepromTest .....
PASS
Starting test: i2cTest .....
ERROR: ioctl: "QSFP0" op(1)=READ WITH STOP bus=33 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP1" op(1)=READ WITH STOP bus=32 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP2" op(1)=READ WITH STOP bus=31 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP3" op(1)=READ WITH STOP bus=30 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP4" op(1)=READ WITH STOP bus=29 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP5" op(1)=READ WITH STOP bus=28 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP6" op(1)=READ WITH STOP bus=40 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP7" op(1)=READ WITH STOP bus=39 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP8" op(1)=READ WITH STOP bus=38 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP9" op(1)=READ WITH STOP bus=37 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP10" op(1)=READ WITH STOP bus=36
address=0x50 offset=0 U#= length=1
ERROR: ioctl: "QSFP11" op(1)=READ WITH STOP bus=34
address=0x50 offset=0 U#= length=1
ERROR: ioctl: "QSFP0" op(1)=READ WITH STOP bus=49 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP3" op(1)=READ WITH STOP bus=46 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP4" op(1)=READ WITH STOP bus=45 address=0x50
offset=0 U#= length=1
ERROR: ioctl: "QSFP5" op(1)=READ WITH STOP bus=44 address=0x50
offset=0 U#= length=1
i2cTest .....
FAIL
macPhyRegTest .....
PASS
Starting test: pcieScanTest .....
22 PCI devices installed out of 22
pcieScanTest .....
PASS
portcardBcmIdTest .....
PASS
Starting test: portcardBoardRevisionTest .....
+ Access Test for BCM unit 0 : PASSED
+ Access Test for BCM unit 1 : PASSED
+ Access Test for BCM unit 2 : PASSED
portcardBoardRevisionTest .....
PASS
Starting test: qsfpOpticsTest .....
ERROR: Qsfp Module:12 is not present
ERROR: Qsfp Module:13 is not present
ERROR: Qsfp Module:14 is not present
ERROR: Qsfp Module:15 is not present
ERROR: Qsfp Module:16 is not present
ERROR: Qsfp Module:17 is not present
ERROR: Qsfp Module:18 is not present
ERROR: Qsfp Module:19 is not present

```

```

ERROR: Qsfp Module:20 is not present
ERROR: Qsfp Module:21 is not present
ERROR: Qsfp Module:22 is not present
ERROR: Qsfp Module:23 is not present
ERROR: Qsfp Module:24 is not present
ERROR: Qsfp Module:27 is not present
ERROR: Qsfp Module:28 is not present
ERROR: Qsfp Module:29 is not present
qsfpOpticsTest .....
FAIL
qsfpPhyTest .....
PASS
rtcTest .....
PASS
sataSsdTest .....
PASS
Starting test: temperatureTest .....
Thermal Monitor Diodes:
Diode[0] temperature 38.0 C
Diode[1] temperature 39.4 C
Diode[2] temperature 39.1 C
Diode[4] temperature 38.9 C
Port card[0]:
Average temperature 50.2 C, maximum 53.6 C
Port card[1]:
Average temperature 48.7 C, maximum 51.4 C
Port card[2]:
Average temperature 48.8 C, maximum 50.9 C
Ethernet MAC temperature 50.0 C
temperatureTest .....
PASS

----- Group Test Statistics -----
Total      : 11
Passed     : 9
Failed     : 2
Elapsed time : 00H:00M:18S
Stop reason  : after completion
----- Failed tests (level, times) -----
              i2cTest (0, 1)
              qsfpOpticsTest (0, 1)

```

show diag information

Display the status of offline diagnostic tests on a switch.

Z9500

Syntax	show diag information
Defaults	None.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the <code>verbose</code> option.
7.7.1.0	Introduced on the S-Series.

**Usage
Information**

Use the `show diag information` command to view the progress of offline diagnostics on Z9500 CPUs: line-card processors (Linecard slots 0 to 2), Control Processor (Linecard slot 3), and Route Processor (Linecard slot 4).

**Example:
Before offline
diagnostics are
run on a switch**

```
Dell# show diag information
Diag information:
Diag software image version:
9.5(0.1)
-----
Linecard slot 0:      No card diags executed yet (Card
Offline).
Linecard slot 1:      No card diags executed yet (Card
Offline).
Linecard slot 2:      No card diags executed yet (Card
Offline).
Linecard slot 3:      No card diags executed yet (Card
Offline).
-----
```

**Example: After
offline
diagnostics are
run on a switch**

```
Dell# show diag information
Diag information:
Diag software image version:
9.5(0.1)
-----
Linecard slot 0:      Card diags are done (Card Offline).
Linecard slot 1:      Card diags are done (Card Offline).
Linecard slot 2:      Card diags are done (Card Offline).
Linecard slot 3:      Card diags are done (Card Offline).
-----
```

show diag testcase

Display the offline diagnostic tests available for the Z9500 CPUs at each level.

Z9500

Syntax

```
show diag testcase {all | {{cp | rp | linecard} unit-id}
[alllevels | level0 | level1 | level2]}
```

Parameters

all

Enter the keyword `all` to display the complete suite of offline diagnostic tests available on the Z9500.

cp <i>unit-id</i>	Enter the <code>cp <i>unit-id</i></code> parameters to display only the offline diagnostic tests available on the Control Processor CPU. The Control Processor CPU ID is 0.
rp <i>unit-id</i>	Enter the <code>rp <i>unit-id</i></code> parameters to display only the offline diagnostic tests available on the Route Processor CPU. The Route Processor CPU ID is 0.
linecard <i>unit-id</i>	Enter the <code>linecard <i>unit-id</i></code> parameters to display only the offline diagnostic tests available for a specified line card. The range of line-card CPU IDs is from 0 to 2. Each line-card CPU processes packets on the corresponding Z9500 line card; for example, line-card CPU 1 processes packets on line card 1.
alllevels	Enter the keyword <code>alllevels</code> to display the the complete set of offline diagnostic tests.
level0	Enter the keyword <code>level0</code> to display only the Level 0 diagnostic tests. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword <code>level1</code> to display only the Level 1 diagnostic tests. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, ports are shut down automatically.
level2	Enter the keyword <code>level2</code> to display only the Level 2 diagnostic tests. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.

Defaults	Display the complete set of offline diagnostic tests available at all levels.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the <code>verbose</code> option.
7.7.1.0	Introduced on the S-Series.

Usage Information

Offline diagnostics tests are grouped into three levels:

- Level 0 — Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
- Level 1 — A smaller set of diagnostic tests. Level 1 diagnostics perform status/self-test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, or EEPROM) wherever possible.
- Level 2 — The full set of diagnostic tests. Level 2 diagnostics are used primarily for on-board Loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.

Example

```

Dell# show diag testcase linecard 0
-----
L2    L3    IA
      eepromTest: ALL    RUN    YES    YES
NO    NO    NO
      i2cTest: ALL    RUN    YES    YES
NO    NO    NO
      lcFullIxiaSnakeTest: ALL    RUN    NO    NO
NO    NO    YES
      macPhyRegTest: ALL    RUN    YES    YES
NO    NO    NO
      partyLinkStatusTest: ALL    RUN    NO    YES
NO    NO    NO
      pcieScanTest: ALL    RUN    YES    NO
NO    NO    NO
      portcardBcmIdTest: ALL    RUN    YES    NO
NO    NO    NO
      portcardBoardRevisionTest: ALL    RUN    YES    NO
NO    NO    NO
      portcardHiGigLinkStatusTest: ALL    RUN    NO    YES
NO    NO    NO
      portcardIxiaTrafficCmd: ALL    RUN    NO    NO
NO    NO    YES
      portcardPortStats: ALL    RUN    NO    NO
NO    NO    YES
      portcardXELinkStatusTest: ALL    RUN    NO    YES
NO    NO    NO
      qsfpOpticsTest: ALL    RUN    YES    YES
NO    NO    NO
      qsfpPhyTest: ALL    RUN    YES    YES
NO    NO    NO
      qsfpPresenceTest: ALL    RUN    NO    YES

```

NO	NO	NO				
			qsfpReadInterruptTest:	ALL	RUN	NO
NO	NO	YES				NO
			qsfpReadModeTest:	ALL	RUN	NO
NO	NO	YES				NO
			rtcTest:	ALL	RUN	YES
NO	NO	NO				YES
			sataSsdTest:	ALL	RUN	YES
NO	NO	NO				YES
			temperatureTest:	ALL	RUN	YES
NO	NO	NO				NO

Buffer Tuning Commands

This section describes the buffer tuning commands supported on the switch.

 **WARNING: Reconfiguring the buffer allocations is a sensitive operation. Do not use any buffer tuning command without first contacting the Dell Networking Technical Assistance Center (TAC).**

buffer-profile (Configuration)

Create a buffer profile that can be applied to an interface.

Z9500

Syntax	buffer-profile {fp csf} profile-name {global {1Q 4q}}		
Parameters			
	fp	Enter the keyword fp to create a buffer profile for the Field Processor.	
	csf	Enter the keyword csf to create a buffer profile for the Switch Fabric Processor.	
	profile-name	Create a name for the buffer profile,	
	global	Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.	
	1Q	Enter the keyword 1Q to choose a pre-defined buffer profile for single queue (for example, non-QoS) applications.	
	4Q	Enter the keyword 4q to choose a pre-defined buffer profile for four queue (for example, QoS) applications.	
Defaults	Dynamic		
Command Modes	CONFIGURATION		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .		
	The following is a list of the Dell Networking OS version history for this command.		

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Changed the default value from global 4q to Dynamic.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
7.8.1.0	Added the <code>global</code> keyword.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.

Usage Information

The `buffer-profile global` command fails if you have already applied a custom buffer-profile on an interface. Similarly, when you configure `buffer-profile global`, you cannot not apply buffer-profile on any interface.

If the default buffer-profile is active, Dell Networking OS displays an error message instructing you to remove the default configuration using the `no buffer-profile global` command.

Reload the system for the global buffer-profile to take effect.

Hardware Commands

The hardware commands supported on the switch allow you to display information from a hardware sub-component or ASIC.

clear control-traffic

Clear control-traffic statistics from a Z9500 CPU.

Z9500

Syntax	<code>clear control-traffic {all cp-switch linecard slot-id portset port-pipe} counters</code>	
Parameters	cp-switch	Enter the keyword <code>cp-switch</code> to clear the counters for control traffic on the control plane.
	linecard slot-id portset port-pipe	Enter the slot ID and port pipe to clear the counters for control traffic on a specified Z9500 line card and port set. The range of Z9500 slot IDs is from 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.
	all	Enter the keyword <code>all</code> to clear control-traffic statistics on the control plane and all line cards.

Defaults	None.
Command Modes	EXEC Privilege
Example	Dell# clear control-traffic cp-switch counters
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the ES-Series.

clear hardware

Clear statistics from a specified hardware component.

Z9500

Syntax

```
clear hardware {cp {cpu {data-plane | i2c | sata-interface}
statistics} | cp-switch {counters} | linecard slot-id {counters
| cpu {data-plane | i2c | sata-interface} statistics} | unit
unit-num {counters} | party-bus {port port-num statistics |
all} | rp {cpu {data-plane | i2c | sata-interface} statistics}
| sfm sfm-unit-num {counters}}
```

Parameters

cp	Enter the keywords <code>cp</code> with a command option to clear the hardware statistics for the Control Processor. The command options are: <code>cpu data-plane statistics</code>: Clears data-plane statistics, including the high-Gigabit Ethernet (HiGig) port statistics with input/output counters to which the stacking module is connected. <code>cpu i2c statistics</code>: Clears active i2c-address statistics. <code>cpu sata-interface statistics</code>: Clears sata-interface error counter statistics.
cp-switch	Enter the keyword <code>cp-switch</code> with a command option to clear the hardware statistics for control-plane and protocol control traffic. The command options are: <code>counters</code>: Clears the counters for control-plane and protocol control packets to troubleshoot an error condition.

linecard <i>slot-id</i>	Enter the <code>linecard <i>slot-id</i></code> parameters with a command option to clear the hardware statistics for a specified Z9500 line card. The range of slot IDs is from 0 to 2. The command options are: • <code>counters</code>: Clears traffic counters on line-card ports. • <code>cpu data-plane statistics</code>: Clears data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected. • <code>cpu i2c statistics</code>: Clears active i2c-address statistics. • <code>cpu sata-interface statistics</code>: Clears sata-interface error counter statistics.
unit <i>unit-num</i>	Enter the <code>unit <i>unit-num</i></code> parameters with a command option to clear hardware statistics for a specified NPU. The range of NPU numbers is 0 to 3. The command options are: • <code>counters</code>: Clears the packets counters.
party-bus	Enter the keyword <code>party-bus</code> with a command option to clear hardware statistics for the party bus that links Z9500 CPUs. The command options are: • <code>port <i>port-num</i> statistics</code>: Clears statistics on a specified party-bus internal port. • <code>port all</code>: Clear statistics on all party-bus internal ports.
rp	Enter the keyword <code>rp</code> with a command option to clear hardware statistics for the Route Processor. The command options are: • <code>cpu data-plane statistics</code>: Clears data-plane statistics, including the HiGig port statistics with input/output counters. • <code>cpu i2c statistics</code>: Clears active i2c-address statistics. • <code>cpu sata-interface statistics</code>: Clears sata-interface error counter statistics.
sfm <i>sfm-unit-num</i>	Enter the keyword <code>sfm</code> with an Switch Fabric Module (SFM) unit number and a command option to clear hardware statistics from the specified SFM on the Z9500. The range of SFM unit numbers is from 0 to 5. The command options are: • <code>counters</code>: Clears the traffic counters.

Defaults none

Command Modes	EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.0	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.0	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
7.8.1.0	Introduced on the S-Series.												
Related Commands	show hardware — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.												

clear hardware system-flow

Clear system-flow statistics from a specified line card.

Z9500

Syntax	<code>clear hardware system-flow layer2 linecard slot-id port-set port-pipe counters</code>	
Parameters	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to identify the Z9500 line card on which you want to clear system-flow statistics. The range of slot IDs is from 0 to 2.
	port-set port-pipe counters	Enter the keywords <code>port-set</code> along with a port-pipe number, then the keyword <code>counters</code> to clear the system-flow counters on the selected port-pipe. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Related Commands [show hardware](#) — displays the data plane or management plane input and output statistics for a specified hardware component.

remote-exec

Debug and troubleshoot switch hardware using remote commands.



WARNING: Use the `remote-exec` command only with the guidance of an engineer from Dell Networking Technical Support.

Z9500

Syntax	<code>remote-exec {cp rp linecard slot-id} hw-command</code>	
Parameters	cp	Enter the keyword <code>cp</code> to troubleshoot Control Processor CPU operation.
	rp	Enter the keyword <code>rp</code> to troubleshoot Route Processor CPU operation.
	linecard slot-id	Enter the <code>linecard slot-id</code> to troubleshoot line-card CPU operation. The range of line-card slot IDs is from 0 to 2. Each line-card CPU processes packets on the corresponding Z9500 line card.
	hw-command	Enter the debug command that Dell Networking Tech Support gives you.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.

	Version	Description
	9.2(0.0)	Modified the <code>drops</code> keyword range, unit keyword <code>range</code> and added the <code>buffer</code> and <code>cpu management statistics</code> options.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.5	Added i2c statistics and sata-interfaces statistics.
	8.3.11.4	Added user port information.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.7.1.0	Introduced on the S-Series.
Usage Information	Use the <code>remote-exec</code> command to remotely execute a command on the Route Processor and line-card (LP) processor from the Control Processor.	
Related Commands	show hardware — displays information on hardware components.	

show control-traffic

Display information about the control traffic transmitted on a Z9500 CPU: Route Processor, Control Processor, or line card.

Z9500

Syntax	<code>show control-traffic {cp rp linecard slot-id} counters</code>	
Parameters	cp	Enter the keyword <code>cp</code> to display control-traffic information from the Control Processor CPU.
	rp	Enter the keyword <code>rp</code> to display control-traffic information from the Route Processor CPU.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to display control-traffic information from the specified line-card processor. The range of Z9500 slot IDs is from 0 to 2.
Defaults	None.	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the ES-Series.

Example Dell# show control-traffic counters

show hardware

Display input and output traffic statistics and other operational information about a specified hardware component.

Z9500

Syntax

```
show hardware {cp {cpu {data-plane | i2c | management | sata-
interface} statistics} |

cp-switch {counters | details | drops | port-stats | register |
table-dump} |

linecard slot-id {buffer {total-buffer | unit unit-num [port
port-num [queue queue-num]]} |

cpu {data-plane | i2c | management | sata-interface} statistics
|

drops {unit unit-num {port {port-num | port-range}} |

user-port {user-port-num | port-range}} |

unit unit-num {counters | details | ipmc-replication | port-
stats | register | table-dump} |

bp-link-map | bp-link-state | higig unit unit-num [port port-
num]}

party-bus {port port-num statistics | all}

rp {cpu {data-plane | i2c | management | sata-interface}
statistics} |

sfm sfm-unit-num {buffer {total-buffer | unit unit-num {port |
total-buffer}} | counters | details | drops | port-stats |
register | table-dump}}
```

Parameters

- | | |
|-----------|--|
| cp | Enter the keywords cp with a command option to display hardware statistics from the Control Processor. The command options are: |
|-----------|--|
- **cpu data-plane statistics:** Displays data-plane statistics, including the HiGig port statistics with input/

output counters to which the stacking module is connected.

- `cpu i2c statistics`: Displays active i2c-address statistics.
- `cpu management statistics`: Displays management port counters.
- `cpu sata-interface statistics`: Displays sata-interface error counter statistics.

cp-switch

Enter the keyword `cp-switch` with a command option to display hardware statistics for control-plane and protocol control traffic. The command options are:

- `counters`: Displays the counters for control-plane and protocol control packets to troubleshoot an error condition.
- `details`: Displays more detailed information on control-plane and protocol control packet statistics.
- `drops`: Displays the number of internal drops of control-plane and protocol control packets.
- `port-stats`: Displays status about why a control-plane internal port is not brought up to register level.
- `register`: Displays internal control-plane registers.
- `table-dump`: Displays the tables from the bShell.

linecard slot-id

Enter the `linecard slot-id` parameters with a command option to display hardware statistics from the specified line-card ports. The range of line-card slot IDs is from 0 to 2. The command options are:

- `buffer total-buffer statistics`: Displays the total number of buffers allocated for a specified line card.
- `buffer unit unit-num port statistics`: Displays the number of buffers allocated for a specified NPU. The range of port-pipe unit numbers is 0 to 3.
- `buffer unit unit-num total-buffer statistics`: Displays the number of buffers allocated for a specified NPU. The range of NPU numbers is 0 to 3.
- `cpu data-plane statistics`: Displays data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics`: Displays active i2c-address statistics.
- `cpu management statistics`: Displays management port counters for a specified line card.
- `cpu sata-interface statistics`: Displays sata-interface error counter statistics.
- `drops unit unit-num {port {port-num | range}}`: Displays the number of dropped packets on the ports of a specified line-card NPU. The range of NPU numbers is 0 to 3.

- `user-port {user-port-num | port-range}`: Displays statistics on a specified line-card port or range of ports.
- `unit unit-num {counters | details | ipmc-replication | port-stats | register | table-dump}`: Displays statistics on a specified NPU. The range of NPU numbers is 0 to 3. The command options are:
 - `counters`: Displays the traffic counters.
 - `details`: Displays more detailed hardware information.
 - `ipmc-replication`: Displays the multicast IPMC replication table from the bShell.
 - `port-stats`: Displays the internal statistics on a per-port basis.
 - `register`: Displays the line-card internal registers.
 - `table-dump`: Displays the tables from the bShell.
- `bp-link-map`: Displays the backplane links (between leaf/port and spine/fabric) on a specified line card.
- `bp-link-state`: Displays the status of the backplane links on a specified line card.
- `hg-stats unit unit-num port port-num`: Displays input and output statistics for a HiGig port (NPU port number) on a specified line card.

party-bus

Enter the keyword `party-bus` with a command option to display hardware statistics from the party bus that links Z9500 CPUs. The command options are:

- `port port-num statistics`: Displays statistics on a specified party-bus internal port.
- `port all`: Displays statistics on all party-bus internal ports.

rp

Enter the keyword `rp` with a command option to display hardware statistics from the Route Processor. The command options are:

- `cpu data-plane statistics`: Displays data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics`: Displays active i2c-address statistics.
- `cpu management statistics`: Displays management port counters.
- `cpu sata-interface statistics`: Displays sata-interface error counter statistics.

sfm sfm-unit-num

Enter the keyword `sfm` with an Switch Fabric Module (SFM) unit number and a command option to display hardware

statistics from the specified SFM on the Z9500. The range of SFM unit numbers is from 0 to 5. The command options are:

- `buffer {total-buffer | unit unit-num {port port-num | total-buffer}}`: Displays buffer statistics from the total SFM buffer or from a specified SFM unit. The range of SFM unit ID numbers is from 0 to 5. The range of SFM unit ports is from 1 to 128.
- `counters`: Displays the counters for SFM traffic to troubleshoot an error condition.
- `details`: Displays more detailed information on control-plane and protocol control packet statistics.
- `drops`: Displays the number of internal drops on the specified SFM unit.
- `port-stats`: Displays status about why an SFM port is not brought up to register level.
- `register`: Displays the internal registers for each switch fabric.
- `table-dump`: Displays the tables from the bShell.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Modified the <code>drops</code> keyword range, unit keyword range and added the <code>buffer</code> and <code>cpu management statistics</code> options.
8.3.19.0	Introduced on the S4820T.
8.3.11.5	Added i2c statistics and sata-interfaces statistics.
8.3.11.4	Added user port information.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Modified the <code>stack-port</code> keyword range expanded from 49-52 to 0-52; output modified for the <code>cpu data-plane statistics</code> option; the following options were added: <code>drops [unit 0-1 [port 0-27]]</code> and <code>unit 0-1</code>

Version	Description
	{counters details port-stats [detail] register}
7.7.1.0	Introduced on the S-Series.

**Example
(Linecard CPU
Dataplane:
Statistics)**

```
Dell#show hardware linecard 2 cpu data-plane statistics
```

```
HANSKVILLE Mib Counters:
TR 64 byte frames = 3
TR 127 byte frames = 358
TR 255 byte frames = 1363
TR 511 byte frames = 1934
TR 1023 byte frames = 18
TR MAX Byte frames = 6202
TR MGv Frames = 0
Bytes Transmitted = 0
Frames Transmitted = 9878
Mcast Frames Transmitted = 0
Bcast Frames Transmitted = 4
Pause Frames Transmitted = 0
Deferred Transmits = 0
Excessive Deferred Transmits = 0
TX single collisions = 0
TX multiple collisions = 0
TX late collisions = 0
TX Excessive collisions = 0
TX total collisions = 0
TX Drops = 0
TX Jabber = 0
TX FCS errors = 0
TX Control frames = 0
TX oversize frames = 0
TX undersize frames = 0
TX fragments = 0
Bytes received = 0
Frames received = 2868
Bcast frames recvd = 24
Mcast frames recvd = 0
Control frames received = 0
Pause frames received = 0
FCS Errors = 0
Alignment errors = 0
Undersize frames recvd = 0
Oversize frames recvd = 0
Fragments = 0
Jabber = 0
Dropped Frames = 0
Under/oversized frames = 0
FLR frames = 0
RCDE frames = 0
RCSE frames = 0
```

**Example
(Party-Bus
Port: Statistics)**

```
Dell#show hardware party-bus port 0 statistics
```

```
Party Bus Transmit Counters for port 0:
Tx Octets = 231162055
Tx Drop Packets = 0
tx_q0_pkts = 303459
tx_q1_pkts = 0
tx_q2_pkts = 0
```

```

tx_q3_pkts = 0
tx_q4_pkts = 0
tx_q5_pkts = 0
tx_broad_pkts = 6178
tx_multi_pkts = 852
tx_uni_pkts = 296429
tx_pause_pkts = 0
tx_cols = 0
tx_single_cols = 0
tx_multi_cols = 0
tx_late_cols = 0
tx_excess_cols = 0
tx_deferred = 0
tx_discarded = 0
Party Bus Receive Counters for port 0:
Rx Octets = 219885483
Rx Undersize Packets = 0
Rx Oversize Packets = 0
Rx Pause Packets = 0
Rx 64 Octet Packets = 115814
Rx 65to127octets Packets = 13278
Rx 128to255octets Packets = 523
Rx 256to511octets Packets = 3382
Rx 512to1023octets Packets = 2530
Rx 1024toMaxoctets Packets = 141767
Rx Jabbers = 0
Rx align errors = 0
Rx fcs errors = 0
Rx good octets = 219885483
Rx Drop pkts = 0
Rx Unicast Packets = 277279
Rx Multicast Packets = 0
Rx Broadcast Packets = 15
Rx Source Address Changes = 1
Rx Fragments = 0
Rx Jumbo Packets = 0
Rx Symbol Errors = 0
Rx In Range Errors = 0
Rx OutofRange Errors = 0

```

**Example
(Linecard:
Drops)**

```

Dell#show hardware linecard 2 drops

UNIT No: 0
Total Ingress Drops      : 3235
Total IngMac Drops       : 0
Total Mmu Drops          : 0
Total EgMac Drops        : 0
Total Egress Drops       : 0

```

**Example
(Linecard Unit:
Drops)**

```

Dell#show hardware linecard 2 drops unit 0

UserPort  PortNumber  Ingress Drops  IngMac Drops
Total Mmu Drops  EgMac Drops    Egress Drops
0          1          0
0          0          0          0
4          5          0
0          0          0          0
8          9          0
0          0          0          0
12         13         3258
0          0          0          0
16         17         0

```


0	0	0	0
17	18	0	
0	0	0	0
18	19	0	
0	0	0	0
19	20	0	
0	0	0	0
20	21	0	
0	0	0	0
21	22	0	
0	0	0	0
22	23	0	
0	0	0	0
23	24	0	
0	0	0	0
24	25	0	
0	0	0	0
28	29	0	
0	0	0	0
32	33	0	
0	0	0	0
36	37	0	
0	0	0	0
40	41	0	
0	0	0	0
44	45	0	
0	0	0	0
Internal	50	0	
0	0	0	0
Internal	51	0	
0	0	0	0
Internal	52	0	
0	0	0	0
Internal	53	0	
0	0	0	0
Internal	54	0	
0	0	0	0
Internal	55	0	
0	0	0	0
Internal	56	0	
0	0	0	0
Internal	57	0	
0	0	0	0
Internal	58	0	
0	0	0	0
Internal	59	0	
0	0	0	0
Internal	60	0	
0	0	0	0
Internal	61	0	
0	0	0	0

**Example
(Linecard Unit
Port: Drops)**

```

Dell#show hardware linecard 2 drops unit 0 port 12

Drops in UserPort 12:
--- Ingress Drops      ---
Ingress Drops           : 3299
IBP CBP Full Drops      : 0
PortSTPnotFwd Drops     : 0
IPv4 L3 Discards        : 0
Policy Discards          : 0
Packets dropped by FP    : 3299
(L2+L3) Drops           : 0

```

```

Port bitmap zero Drops      : 0
Rx VLAN Drops              : 0
  --- Ingress MAC counters---
Ingress FCSDrops           : 0
Ingress MTUExceeds         : 0
  --- MMU Drops            ---
HOL DROPS (TOTAL)          : 0
HOL DROPS on COS0          : 0
HOL DROPS on COS1          : 0
HOL DROPS on COS2          : 0
HOL DROPS on COS3          : 0
HOL DROPS on COS4          : 0
HOL DROPS on COS5          : 0
HOL DROPS on COS6          : 0
HOL DROPS on COS7          : 0
HOL DROPS on COS8          : 0
HOL DROPS on COS9          : 0
HOL DROPS on COS10         : 0
HOL DROPS on COS11         : 0
HOL DROPS on COS12         : 0
HOL DROPS on COS13         : 0
HOL DROPS on COS14         : 0
HOL DROPS on COS15         : 0
HOL DROPS on COS16         : 0
HOL DROPS on COS17         : 0
HOL DROPS on COS18         : 0
HOL DROPS on COS19         : 0
HOL DROPS on COS20         : 0
TxPurge CellErr           : 0
Aged Drops                 : 0
  --- Egress MAC counters---
Egress FCS Drops           : 0
  --- Egress FORWARD PROCESSOR Drops ---
IPv4 L3UC Aged & Drops     : 0
TTL Threshold Drops        : 0
INVALID VLAN CNTR Drops    : 0
L2MC Drops                 : 0
PKT Drops of ANY Conditions : 0
Hg MacUnderflow            : 0
TX Err PKT Counter         : 0
  --- Error counters---
Internal Mac Transmit Errors : 0
Unknown Opcodes            : 0
Internal Mac Receive Errors  : 0

```

Example
(Linecard Unit:
Port-Stats)

```

Dell#show hardware linecard 2 unit 0 port-stats
      ena/  speed/ link auto  STP          lrn
inter  max  loop
      port link duplex scan neg?  state  pause  discred
ops    face frame back
      xe0  !ena  40G FD  SW  No  Forward          Tag
F      CR4  1550
      xe1  !ena  40G FD  SW  No  Forward          Tag
F      XGMII 1550
      xe2  !ena  40G FD  SW  No  Forward          Tag
F      XGMII 1550
      xe3  up    40G FD  SW  No  Forward          Tag
F      SR4  1550
      xe4  down  10G FD  SW  No  Forward          Tag
F      SFI  1550
      xe5  down  10G FD  SW  No  Forward          Tag
F      SFI  1550
      xe6  down  10G FD  SW  No  Forward          Tag

```

F	SFI	1550						
	xe7	down	10G	FD	SW	No	Forward	Tag
F	SFI	1550						
	xe8	up	10G	FD	SW	No	Forward	Tag
F	SFI	1550						
	xe9	!ena	10G	FD	SW	No	Forward	Tag
F	SFI	1550						
	xe10	!ena	10G	FD	SW	No	Forward	Tag
F	SFI	1550						
	xe11	!ena	10G	FD	SW	No	Forward	Tag
F	SFI	1550						
	xe12	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	xe13	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	xe14	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	xe15	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	xe16	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	xe17	!ena	40G	FD	SW	No	Forward	Tag
F	XGMII	1550						
	ge0	up	1G	FD	SW	No	Forward	None
FA	GMII	16360						
	hg0	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg1	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg2	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg3	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg4	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg5	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg6	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg7	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg8	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg9	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg10	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						
	hg11	up	42G	FD	SW	No	Forward	None
F	XGMII	16360						

**Example
(Linecard Unit:
Register)**

```

Dell#show hardware linecard 2 unit 0 register
0x77120000 ARB_RAM_DBGCTRL.ipipe0 = 0x00000000
0x04000134 ASF_PORT_CFG.cpu0 = 0x00000000
0x04000107 ASF_PORT_CFG.xe0 = 0x0000001c
0x04000109 ASF_PORT_CFG.xe1 = 0x0000001c
0x0400010b ASF_PORT_CFG.xe2 = 0x0000001c
0x04000141 ASF_PORT_CFG.xe3 = 0x0000001c
0x0400014a ASF_PORT_CFG.xe4 = 0x0000000c
0x0400014b ASF_PORT_CFG.xe5 = 0x0000000c
0x0400014c ASF_PORT_CFG.xe6 = 0x0000000c
0x0400014d ASF_PORT_CFG.xe7 = 0x0000000c
0x0400014e ASF_PORT_CFG.xe8 = 0x0000000c
0x0400014f ASF_PORT_CFG.xe9 = 0x0000000c

```

```

0x04000150 ASF_PORT_CFG.xe10 = 0x0000000c
0x04000151 ASF_PORT_CFG.xe11 = 0x0000000c
0x04000106 ASF_PORT_CFG.xe12 = 0x0000001c
0x04000108 ASF_PORT_CFG.xe13 = 0x0000001c
0x0400010a ASF_PORT_CFG.xe14 = 0x0000001c
0x04000140 ASF_PORT_CFG.xe15 = 0x0000001c
0x04000142 ASF_PORT_CFG.xe16 = 0x0000001c
0x04000143 ASF_PORT_CFG.xe17 = 0x0000001c
0x0400010c ASF_PORT_CFG.ge0 = 0x00000007
0x04000144 ASF_PORT_CFG.hg0 = 0x0000001d
0x04000145 ASF_PORT_CFG.hg1 = 0x0000001d
0x04000147 ASF_PORT_CFG.hg2 = 0x0000001d
0x04000146 ASF_PORT_CFG.hg3 = 0x0000001d
0x04000149 ASF_PORT_CFG.hg4 = 0x0000001d
0x04000148 ASF_PORT_CFG.hg5 = 0x0000001d
0x04000100 ASF_PORT_CFG.hg6 = 0x0000001d
0x04000101 ASF_PORT_CFG.hg7 = 0x0000001d
0x04000103 ASF_PORT_CFG.hg8 = 0x0000001d
0x04000102 ASF_PORT_CFG.hg9 = 0x0000001d
0x04000105 ASF_PORT_CFG.hg10 = 0x0000001d
0x04000104 ASF_PORT_CFG.hg11 = 0x0000001d
0x04000174 ASF_PORT_CFG.lb0 = 0x00000000
0x77000000 AUX_ARB_CONTROL.ipipe0 = 0x00000012
0x77010000 AUX_ARB_CONTROL_2.ipipe0 = 0x64ff40a3
0x16004a00 BFD_RX_ACH_TYPE_CONTROL0.ipipe0 = 0x00570021
0x16004b00 BFD_RX_ACH_TYPE_CONTROL1.ipipe0 = 0x00000007
0x16004c00 BFD_RX_ACH_TYPE_MPLSTP.ipipe0 = 0x00000000
0x16005300 BFD_RX_ACH_TYPE_MPLSTP1.ipipe0 = 0x0000000000000000
0x0a009900 BFD_RX_UDP_CONTROL.ipipe0 = 0x0ec812b0
0x16004900 BFD_RX_UDP_CONTROL_1.ipipe0 = 0x0ec812b0
0x26001500 BKPMETERINGDISCSTATUS0.mmu0 = 0x0000000000000000
0x26001600 BKPMETERINGDISCSTATUS1.mmu0 = 0x0000000000000000
0x26001000 BKPMETERINGWARNSTATUS0.mmu0 = 0x0000000000000000
0x26001100 BKPMETERINGWARNSTATUS1.mmu0 = 0x0000000000000000
0x32000900 BST_HW_SNAPSHOT_EN.mmu0 = 0x00000000
0x32000800 BST_SNAPSHOT_ACTION_EN.mmu0 = 0x00000000
0x32000700 BST_TRACKING_ENABLE.mmu0 = 0x00000000
0x56002000 BUF_CFG(0).mmu0 = 0x00000000
0x56002001 BUF_CFG(1).mmu0 = 0x00000000
0x56002002 BUF_CFG(2).mmu0 = 0x00000000
0x56002003 BUF_CFG(3).mmu0 = 0x00000000
0x56002004 BUF_CFG(4).mmu0 = 0x00000000
0x56002005 BUF_CFG(5).mmu0 = 0x00000000
0x56002006 BUF_CFG(6).mmu0 = 0x00000000
0x56002007 BUF_CFG(7).mmu0 = 0x00000000
0x56002008 BUF_CFG(8).mmu0 = 0x00000000
0x56002009 BUF_CFG(9).mmu0 = 0x00000000
0x5600200a BUF_CFG(10).mmu0 = 0x00000000
0x5600200b BUF_CFG(11).mmu0 = 0x00000000
0x5600200c BUF_CFG(12).mmu0 = 0x00000000
0x5600200d BUF_CFG(13).mmu0 = 0x00000000
0x5600200e BUF_CFG(14).mmu0 = 0x00000000
0x5600200f BUF_CFG(15).mmu0 = 0x00000000
0x36000200 CBL_ATTRIBUTE(0).ipipe0 = 0x00000000
0x36000201 CBL_ATTRIBUTE(1).ipipe0 = 0x00000000
0x36000202 CBL_ATTRIBUTE(2).ipipe0 = 0x00000000
0x36000203 CBL_ATTRIBUTE(3).ipipe0 = 0x00000000
0x37040000 CCM_INTERRUPT_CONTROL.ipipe0 = 0x00000000
0x37030000 CCM_READ_CONTROL.ipipe0 = 0x00000000
0x22001200 CCPMEMDEBUG.mmu0 = 0x00000000
0x22001000 CCP_STS.mmu0 = 0x00000003
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl0 = 0x0000000000000001
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl1 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl2 = 0x0000000000000000

```

```

0x02001a00 CELL_ASM_0_CONTROL.pgw_c13 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_c14 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_c15 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_c16 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_c17 = 0x0000000000000000
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c10 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c11 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c12 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c13 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c14 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c15 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c16 =
0x000000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_c17 =
0x000000000000318c6
0x12002000 CELL_LINK_MEM_DEBUG_TM.mmu0 = 0x00000000
0x1e001000 CFAPBANKFULL(0).mmu0 = 0x000007ff
0x1e001001 CFAPBANKFULL(1).mmu0 = 0x000007ff
0x1e001002 CFAPBANKFULL(2).mmu0 = 0x000007ff
0x1e001003 CFAPBANKFULL(3).mmu0 = 0x000007ff
0x1e001004 CFAPBANKFULL(4).mmu0 = 0x000007ff
0x1e001005 CFAPBANKFULL(5).mmu0 = 0x000007ff
0x1e001006 CFAPBANKFULL(6).mmu0 = 0x000007ff
0x1e001007 CFAPBANKFULL(7).mmu0 = 0x000007ff
0x1e001008 CFAPBANKFULL(8).mmu0 = 0x000007ff
0x1e001009 CFAPBANKFULL(9).mmu0 = 0x000007ff
0x1e00100a CFAPBANKFULL(10).mmu0 = 0x000007ff
0x1e00100b CFAPBANKFULL(11).mmu0 = 0x000007ff
0x1e00100c CFAPBANKFULL(12).mmu0 = 0x000007ff
0x1e00100d CFAPBANKFULL(13).mmu0 = 0x000007ff
0x1e00100e CFAPBANKFULL(14).mmu0 = 0x000007ff
0x1e00100f CFAPBANKFULL(15).mmu0 = 0x000007ff
0x1e003000 CFAPBANKSTATUS(0).mmu0 = 0x00000028
0x1e003001 CFAPBANKSTATUS(1).mmu0 = 0x00000025
0x1e003002 CFAPBANKSTATUS(2).mmu0 = 0x00000022
0x1e003003 CFAPBANKSTATUS(3).mmu0 = 0x00000025
0x1e003004 CFAPBANKSTATUS(4).mmu0 = 0x00000023
0x1e003005 CFAPBANKSTATUS(5).mmu0 = 0x00000023
0x1e003006 CFAPBANKSTATUS(6).mmu0 = 0x00000027
0x1e003007 CFAPBANKSTATUS(7).mmu0 = 0x00000026
0x1e003008 CFAPBANKSTATUS(8).mmu0 = 0x00000027
!----- output truncated -----!

```

**Example
(Linecard Unit:
Counters)**

```

Dell#show hardware linecard 0 unit 1 counters
RUC.cpu0 : 528,687
+528,687
ING_NIV_RX_FRAMES.cpu0 : 528,687
+528,687
TDBG66.cpu0 : 528,687
+528,687
PERQ_PKT(0).cpu0 : 1,172
+1,172
PERQ_PKT(41).cpu0 : 527,515
+527,515
PERQ_BYTE(0).cpu0 : 79,696
+79,696
PERQ_BYTE(41).cpu0 : 35,871,020

```

```

+35,871,020
PERQ_DROP_PKT(0).cpu0      :          217,930
+217,930
PERQ_DROP_PKT(41).cpu0    :          2,186,107,010
+2,186,107,010
PERQ_DROP_BYTE(0).cpu0    :          14,819,240
+14,819,240
PERQ_DROP_BYTE(41).cpu0   :          148,655,276,680
+148,655,276,680
QUEUE_PEAK(0).cpu0        :              224
QUEUE_PEAK(41).cpu0       :              236
RUC.xe0                   :          2,756,973,184
+2,756,973,184
RDBG0.xe0                 :          2,186,634,525
+2,186,634,525
RDBG5.xe0                 :          2,186,634,525
+2,186,634,525
ING_NIV_RX_FRAMES.xe0     :          2,756,973,184
+2,756,973,184
TDBG3.xe0                 :          2,881,121
+2,881,121
TDBG6.xe0                 :          190,692,963,094
+190,692,963,094      12,017,817/s
TDBG10.xe0                :          2,881,121
+2,881,121
R127.xe0                  :          2,756,973,184
+2,756,973,184
RPKT.xe0                  :          2,756,973,184
+2,756,973,184

```

**Example
(Linecard Unit:
Details)**

```

Dell#show hardware linecard 2 unit 0 details

*****

The total no of FP & CSF Devices in the Card is 1
The total no of FP Devices in the Card is 1
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 18
The number of Hg ports in devices 0 is - 12
The CPU Port of the device is 0
The starting unit no the SWF in the device is 0
*****

bcmLinkMonStatusShow: The Current Link Status Is

Front End Link Status      0x00080800 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000
Front End Port Presence    0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000
Backplane Link Status      0xc0000300 0x000c0000
*****

Link Status of all the ports in the Device - 0

The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 13 is TRUE
The linkStatus of Front End Port 17 is FALSE
The linkStatus of Front End Port 18 is FALSE
The linkStatus of Front End Port 19 is FALSE
The linkStatus of Front End Port 20 is FALSE
The linkStatus of Front End Port 21 is TRUE

```

```

The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is FALSE
The linkStatus of Front End Port 24 is FALSE
The linkStatus of Front End Port 25 is FALSE
The linkStatus of Front End Port 29 is FALSE
The linkStatus of Front End Port 33 is FALSE
The linkStatus of Front End Port 37 is FALSE
The linkStatus of Front End Port 41 is FALSE
The linkStatus of Front End Port 45 is FALSE
The linkStatus of Hg Port 50 is TRUE
The linkStatus of Hg Port 51 is TRUE
The linkStatus of Hg Port 52 is TRUE
The linkStatus of Hg Port 53 is TRUE
The linkStatus of Hg Port 54 is TRUE
The linkStatus of Hg Port 55 is TRUE
The linkStatus of Hg Port 56 is TRUE
The linkStatus of Hg Port 57 is TRUE
The linkStatus of Hg Port 58 is TRUE
The linkStatus of Hg Port 59 is TRUE
The linkStatus of Hg Port 60 is TRUE
The linkStatus of Hg Port 61 is TRUE
*****

```

```

Trunk Info for Unit 0 -----
The allocated Trunk ID is - 1024
The PSC is - 9
The Current Trunk ID - 1025
Init Done is - 1
Trunk Valid is - 1
Trunk Port Information
The flags is - 0
The no of ports is - 12
The PSC is - 9
The DLF Index is - -1
The MC Index is - -1
The IPMC Index is - -1
The tm-tp for Index 0 is : -1 | -1
The tm-tp for Index 1 is : -1 | -1
The tm-tp for Index 2 is : -1 | -1
The tm-tp for Index 3 is : -1 | -1
The tm-tp for Index 4 is : -1 | -1
The tm-tp for Index 5 is : -1 | -1
The tm-tp for Index 6 is : -1 | -1
The tm-tp for Index 7 is : -1 | -1
The tm-tp for Index 8 is : -1 | -1
The tm-tp for Index 9 is : -1 | -1
The tm-tp for Index 10 is : -1 | -1
The tm-tp for Index 11 is : -1 | -1

```

```

ModPort Table for Device - 0
For Destination Mod Id 0 Destination Port is 50
For Destination Mod Id 1 Destination Port is 50
For Destination Mod Id 2 Destination Port is 50
For Destination Mod Id 3 Destination Port is 50
For Destination Mod Id 4 Destination Port is 50
For Destination Mod Id 5 Destination Port is 50
For Destination Mod Id 6 Destination Port is 50
For Destination Mod Id 7 Destination Port is 50
For Destination Mod Id 9 Destination Port is 50
For Destination Mod Id 10 Destination Port is 50

```

```
For Destination Mod Id 11 Destination Port is 50
!----- output truncated -----!
```

**Example
(Linecard:
Total-Buffer)**

```
Dell(conf)#show hardware linecard 2 buffer total-buffer
----- Buffer Details for linecard 2 -----
Total Buffers allocated per linecard 61440
```

**Example
(Linecard Unit
Port: Buffer-
Info)**

```
Dell(conf)#show hardware linecard 2 buffer unit 0 port 12
buffer-info
----- Buffer Stats for Unit 0 Port 13 -----
Maximum Shared Limit for the Port: 44537
Default Packet Buffer allocate for the Port: 150
Used Packet Buffer for the Port: 0

Dell(conf)#show hardware linecard 0 buffer unit 0 port 1 queue
1 buffer-info
----- Buffer Stats for Unit 0 Port 1 Queue 1 -----
Maximum Shared Limit: 27371
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
```

**Example
(Linecard:
Backplane
Links)**

```
Dell#show hardware linecard 0 bp-link-map

Back Plane HG Links
-----
```

LinkId	0	1	2	3	4
5	22	23			
NpuId/PortId	0/56	0/57	1/56	1/57	2/56
2/57	0/58	0/59			

LinkId	24	25	26	27	44
45	46	47			
NpuId/PortId	1/58	1/59	2/58	2/59	0/60
0/61	1/60	1/61			

LinkId	48	49	66	67	68
69	70	71			
NpuId/PortId	2/60	2/61	0/50	0/51	1/50
1/51	2/50	2/51			

LinkId	88	89	90	91	92
93	110	111			
NpuId/PortId	0/52	0/53	1/52	1/53	2/52
2/53	0/54	0/55			

LinkId	112	113	114	115
NpuId/PortId	1/54	1/55	2/54	2/55


```
Back Plane GE Links
-----
```

LinkId	138	139	140
NpuId/PortId	0/49	1/49	2/49

**Example
(Linecard:
Backplane-link
Status)**

```
Dell#show hardware linecard 0 bp-link-state

Total valid Links - 39

Valid Link bmp -
0xfc0003f0-000fc000-3f0000fc-0003f000-00380000

Valid Link bmp State -
0xfc0003f0-000fc000-3d0000fc-0003f000-00380000
```

**Example
(Linecard Unit
Port: HiGig Port
Statistics)**

```
Dell#show hardware linecard 0 hg-stats unit 1 port 50
HiGig Port Statistics:
HiGigabitEthernet 0/1/50,
Input Statistics:
    0 packets, 0 bytes
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:
    0 packets, 0 bytes 0 underruns
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts 0 Unicasts
    0 throttles, 0 discarded, 5208131494077267968 collisions
19141612676317184 wredDrops
Rate info (interval 15 seconds):
    Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
    Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
```

**Related
Commands**

[clear hardware system-flow](#) — clears the statistics from selected hardware components.

[show system](#) — displays the current status of all the stack members or a specific member.

show hardware ipv6

Display information about IPv6 ACLs used on a Z9500 line card and port pipe.

Z9500

Syntax

```
show hardware ipv6 {eg-acl | in-acl} linecard slot-id port-set
port-pipe
```

Parameters

eg-acl | in-acl

Enter either the keyword `eg-acl` or the keyword `in-acl` to display ingress or egress ACL data.

linecard slot-id

Enter the linecard `slot-id` parameters to specify a Z9500 line card. The range of slot IDs is from 0 to 2.

	port-set port-pipe	Enter the keywords <code>port-set port-pipe</code> parameters to specify a port pipe (set of ports) on a line card. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show hardware ipv6 eg-acl linecard 0 port-set 0
EID 0x000013ce: gid=0xd,
    slice=0, slice_idx=0, part =0 prio=0x13ce,
flags=0x10202, Installed, Enabled
    tcam: color_indep=0,
    StageEgress
    slice=1, slice_idx=0, part =1 prio=0x13ce,
flags=0x10204, Installed, Enabled
    tcam: color_indep=0,
    Offset: 1 Width: 8
    DATA=0x0000003a
    MASK=0x000000ff
IpType
    Offset: 208 Width: 5
    DATA=0x00000004
    MASK=0x0000000c
L3Routable
    Offset: 166 Width: 1
    DATA=0x00000001
    MASK=0x00000001
OutPort
    Offset: 195 Width: 7
    DATA=0x00000001
    MASK=0x0000007f
    action={act=Drop, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
    policer=
    statistics=NULL

EID 0x0000130d: gid=0xd,
    slice=0, slice_idx=0x1, part =0 prio=0x130d,
flags=0x10202, Installed, Enabled
    tcam: color_indep=0,
    StageEgress
```

```

        slice=1, slice_idx=0x1, part =1 prio=0x130d,
flags=0x10204, Installed, Enabled
        tcam: color_indep=0,
IpType
    Offset: 208 Width: 5
    DATA=0x00000004
    MASK=0x0000000c
L3Routable
    Offset: 166 Width: 1
    DATA=0x00000001
    MASK=0x00000001
OutPort
    Offset: 195 Width: 7
    DATA=0x00000001
    MASK=0x0000007f
    action={act=Drop, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
    policer=
    statistics={stat id 110 slice = 0 idx=4 entries=1}
{Packets}

```

Usage Information	The port-set values are internal port numbers. For a cross reference of the internal and port numbers, refer to the <i>Debugging and Diagnostics</i> chapter in the <i>Dell Networking OS Configuration Guide for the Z9500 System</i> .
--------------------------	--

show hardware layer2

Display information about the Layer 2 ACLs used on a Z9500 line card and port pipe.

Z9500

Syntax	<code>show hardware layer2 {eg-acl in-acl} linecard slot-id port-set number</code>
---------------	--

Parameters	<table border="0"> <tr> <td style="vertical-align: top;">eg-acl in-acl</td> <td>Enter either the keyword <code>eg-acl</code> or the keyword <code>in-acl</code> to display ingress or egress ACL data.</td> </tr> <tr> <td style="vertical-align: top;">linecardslot-id</td> <td>Enter the <code>linecard slot-id</code> parameters to specify a Z9500 line card. The range of slot IDs is from 0 to 2.</td> </tr> <tr> <td style="vertical-align: top;">port-set number</td> <td>Enter the keywords <code>port-set number</code> parameters to specify a port pipe (set of ports) on a line card. The range of port-set numbers is from 0 to 3.</td> </tr> </table>	eg-acl in-acl	Enter either the keyword <code>eg-acl</code> or the keyword <code>in-acl</code> to display ingress or egress ACL data.	linecardslot-id	Enter the <code>linecard slot-id</code> parameters to specify a Z9500 line card. The range of slot IDs is from 0 to 2.	port-set number	Enter the keywords <code>port-set number</code> parameters to specify a port pipe (set of ports) on a line card. The range of port-set numbers is from 0 to 3.
eg-acl in-acl	Enter either the keyword <code>eg-acl</code> or the keyword <code>in-acl</code> to display ingress or egress ACL data.						
linecardslot-id	Enter the <code>linecard slot-id</code> parameters to specify a Z9500 line card. The range of slot IDs is from 0 to 2.						
port-set number	Enter the keywords <code>port-set number</code> parameters to specify a port pipe (set of ports) on a line card. The range of port-set numbers is from 0 to 3.						

Defaults	none
-----------------	------

Command Modes	EXEC Privilege
----------------------	----------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Usage Information

The port-set values are internal port numbers. For a cross reference of the internal and port numbers, refer to the *Debugging and Diagnostics* chapter in the *Dell Networking OS Configuration Guide for the Z9500 System*.

Example

```
Dell#show hardware layer2 acl eg-acl linecard 2 port-set 0
EID 0x000010ce: gid=0x10,
               slice=3, slice_idx=0, part =0 prio=0x10ce,
flags=0x10202, Installed, Enabled
               tcam: color_indep=0,
StageEgress
Color
  Offset: 22 Width: 2
  DATA=0x00000001
  MASK=0x00000003
  action={act=RpDrop, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
  policer=
  statistics={stat id 62 slice = 3 idx=0 entries=1}
{Packets}

EID 0x000010cd: gid=0x10,
               slice=3, slice_idx=0x1, part =0 prio=0x10cd,
flags=0x10202, Installed, Enabled
               tcam: color_indep=0,
StageEgress
OutPort
  Offset: 193 Width: 7
  DATA=0x00000000
  MASK=0x0000007f
  action={act=RpDrop, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
  policer=
  statistics={stat id 63 slice = 3 idx=0 entries=1}
{Packets}

EID 0x000010cc: gid=0x10,
               slice=3, slice_idx=0x2, part =0 prio=0x10cc,
flags=0x10202, Installed, Enabled
               tcam: color_indep=0,
DstMac
  Offset: 90 Width: 48
  DATA=0x00000180 c2000000
  MASK=0x0000ffff ff000000
StageEgress
  action={act=DropCancel, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
  policer=
  statistics={stat id 65 slice = 3 idx=1 entries=1}
```

```
{Packets}  
--More--
```

show hardware layer3

Display Layer 3 ACL or QoS data for a Z9500 line card and port pipe.

Z9500

Syntax	<pre>show hardware layer3 {acl qos} linecard slot-id port-set port-pipe</pre>	
Parameters	acl qos	Enter either the keyword <code>acl</code> or the keyword <code>qos</code> to select between ACL or QoS data.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify a Z9500 line card. The range of slot IDs is from 0 to 2.
	port-set port-pipe	Enter the keywords <code>port-set port-pipe</code> parameters to specify a port pipe (set of ports) on a line card. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show hardware layer3 eg-acl linecard 0 port-set 0  
EID 0x000011b9: gid=0xf,  
             slice=2, slice_idx=0, part =0 prio=0x11b9,  
flags=0x10202, Installed, Enabled  
             tcam: color_indep=0,  
StageEgress  
Color  
  Offset: 5 Width: 2  
  DATA=0x00000001  
  MASK=0x00000003  
  action={act=RpDrop, param0=0(0), param1=0(0),  
param2=0(0), param3=0(0)}
```

```

        policer=
        statistics={stat id 64  slice = 2 idx=1 entries=1}
{Packets}

EID 0x000011b8: gid=0xf,
        slice=2, slice_idx=0x1, part =0 prio=0x11b8,
flags=0x10202, Installed, Enabled
        tcam: color_indep=0,
    StageEgress
    IpType
        Offset: 192 Width: 4
        DATA=0x00000000
        MASK=0x0000000e
    L3Routable
        Offset: 156 Width: 1
        DATA=0x00000001
        MASK=0x00000001
    OutPort
        Offset: 185 Width: 7
        DATA=0x00000005
        MASK=0x0000007f
        action={act=DropCancel, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
        policer=
        statistics={stat id 110  slice = 2 idx=4 entries=1}
{Packets}

EID 0x00001101: gid=0xf,
        slice=2, slice_idx=0x2, part =0 prio=0x1101,
flags=0x10202, Installed, Enabled
        tcam: color_indep=0,
    StageEgress
    IpFrag
        Offset: 7 Width: 2
        DATA=0x00000000
        MASK=0x00000001
    IpType
    Offset: 192 Width: 4
        DATA=0x00000000
        MASK=0x0000000e
    L3Routable
        Offset: 156 Width: 1
        DATA=0x00000001
        MASK=0x00000001
    OutPort
        Offset: 185 Width: 7
        DATA=0x00000005
        MASK=0x0000007f
        action={act=Drop, param0=0(0), param1=0(0),
param2=0(0), param3=0(0)}
        policer=
        statistics={stat id 111  slice = 2 idx=4 entries=1}
{Packets}

```

show hardware system-flow

Display Layer 3 ACL or QoS data for traffic flows on the central switch (aggregated CoPP) or a specified line card and port pipe.

Z9500

Syntax show hardware system-flow layer2 [cp-switch | linecard *slot-id* port-set *port-pipe*]

Parameters	cp-switch	Enter the keyword cp-switch to display information on system flows of control-plane traffic.
	linecard <i>slot-id</i> portset <i>port-pipe</i>	Enter the slot ID and port pipe to display information on system flows on a specified Z9500 line card and port set. The range of Z9500 slot IDs is from 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.

Defaults	none
----------	------

Command Modes	EXEC Privilege
---------------	----------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Usage Information	Use the <code>show hardware system-flow</code> command to display the system flow entries on the central switch (aggregated CoPP) or on a specified set of Z9500 ports. The command output displays statistics on the number of hits for each system flow.
--------------------------	--

[illegible]

```
param3=0 (0) }
```


Stage
--More--

tcpdump

Enable a TCP dump for CPU-bound traffic on the Control and Router Processors..

Z9500

Syntax

```
tcpdump {cp | rp} [capture-duration time | filter expression |  
max-file-count value | packet-count value | snap-length value |  
write-to path]
```

To disable the TCP dump, use the `no tcpdump` command.

Parameters

cp	Enter the keyword <code>cp</code> to perform a dump on traffic processed by the Control Processor CPU.
rp	Enter the keyword <code>rp</code> to perform a dump on traffic processed by the Route Processor CPU.
capture-duration	Enter the time for packet capturing. The timer begins as soon as the command is enabled. The range is 20 to 9000 seconds.
filter	Specify the packet that will be dumped. If no filter is entered, all packets are dumped. Filter expressions usually consist of an id (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier: type, direction, or protocol. Enclose the filter option with double quotes: "port 20." The range is 1 to 100 characters.
max-file-count	Enter the maximum number of 1MB files. The maximum file size for a TCP dump capture is 1MB. When a file reaches 1MB, a new file is created, up to the specified number. The range is 1 to 20.
packet-count	Enter the number of packets to capture. The counter begins as soon as the command is enabled. The range is 10 to 150000.
snap-length	Enter the number of bytes per packet to capture. Use this option to reduce the size of the captured packets, to capture only the needed headers and avoid rest of the data portion of the packet. The range is 0 to 1200.
write-to	Enter the location to save the captured packets. Files can be saved to flash, to FTP, SCP, or TFTP: • <code>flash://filepath</code> • <code>ftp://userid:password@hostip/filepath</code> • <code>scp://userid:password@hostip/filepath</code>

- `tftp://hostip/filepath`

Defaults

TCP dumps are disabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

Use the `tcpdump` command to perform a packet capture on a specified Z9500 CPU: Control Processor (CP) or Route Processor (RP).

You can use the capture-duration timer and the packet-count counter at the same time. The TCP dump stops when the first of the thresholds is met. That means that even if the duration timer is 9000 seconds, if the maximum file count parameter is met first, the dumps stop.

The files saved on the flash are located in the `flash://TCP_DUMP_DIR/Tcpdump_<time_stamp_dir>/directory`. The file name is `tcpdump_*.pcap`. There can be up to 20 `Tcpdump_<time_stamp_dir>` directories. If more than 20 files are created, the oldest is overwritten.

Entering the `no tcpdump` command stops any TCP dump process running in either the Control Processor or Route Processor. The dump stops immediately, without waiting for a threshold to be met.

To stop the TCP dump process running in the CP processor, enter the `no tcpdump cp` command; to stop the TCP dump process running in the RP processor, enter the `no tcpdump rp` command.

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on the configuration policies the network administrators determine.

The Dell Networking OS supports the basic DHCP commands as described in the following sections:

- [Configure a DHCP Server and DHCP Clients](#)
- [Configure Secure DHCP and DHCP Relay](#)

Configure a DHCP Server and DHCP Clients

To configure the system to be a DHCP server and to manually configure DHCP clients, use the following commands.

clear ip dhcp

Reset the DHCP counters.

Z9500

Syntax	<code>clear ip dhcp [binding {address} client statistics {all interface type slot/port}] conflict server statistics]</code>	
Parameters	binding	Enter the keyword <code>binding</code> to delete all entries in the binding table.
	address	Enter the IP address to clear the binding entry for a single IP address.
	client statistics {all interface type slot/port}	Enter the keywords <code>server statistics all</code> to clear all counter information on all DHCP client interfaces on the switch. Enter an interface type and slot/port information to clear DHCP counters on a specified interface. The valid interface types are: • For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
	conflicts	Enter the keyword <code>conflicts</code> to delete all of the log entries created for IP address conflicts.

	server statistics	Enter the keywords <code>server statistics</code> to clear all counter information on the DHCP server.												
Defaults	none													
Command Modes	EXEC Privilege													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820t.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820t.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series and S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820t.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
8.2.1.0	Introduced on the C-Series and S-Series.													
Usage Information	Entering <CR> after the <code>clear ip dhcp binding</code> command clears all the IPs from the binding table.													

debug ip dhcp client events

Activate the debugging and display of log messages on DHCP client interfaces for IP address acquisition, IP address release, and IP address and lease time renewal.

Z9500

Syntax	debug ip dhcp client events [interface <i>type slot/port</i>]	
Parameters	interface <i>typeslot/port</i>	Enter the keyword interface with the interface type and slot/port information to display DHCP event messages for a specified interface. The valid interface types are: - For a 10-Gigabit Ethernet interface, enter the keyword tengigabitethernet. - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version 9.2(1.0)	Description Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# debug ip dhcp client events

Dell(conf-if-fo-2/0)#do show debugging
Dhcp Client :
  DhcpClient Event debugging is on for fortyGigE 2/0

Dell(conf-if-fo-2/0)#ip address dhcp
Dell(conf-if-fo-2/0)#no ip address dhcp

Dell(conf-if-fo-2/0)#do show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 9 Messages Logged, Size
(40960 bytes)
  Trap logging: level informational
    Logging to 10.10.10.4
    Logging to 10.1.2.4
    Logging to 172.31.1.4
    Logging to 133.33.33.4
    Logging to 172.16.1.162
  Last logging buffer cleared: Jan 7 01:38:04
Jan 7 01:38:42: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_EVT: Interface Fo 2/0 :DHCP DISABLED CMD sent to
FTOS in state START
Jan 7 01:38:41: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_EVT: Interface Fo 2/0 :Transitioned to state START
Jan 7 01:38:41: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_EVT: Interface Fo 2/0 :DHCP DISABLE CMD Received
in state BOUND
Jan 7 01:38:07: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_EVT: Interface Fo 2/0 :DHCP ENABLE CMD Received
in state START

Message                               Sent
BOOTREPLY                             0
DHCPOFFER                             10
DHCPACK                               16
DHCPNAK                               0
```

debug ip dhcp client packets

Activate the debugging and display of log messages for DHCP packets sent and received on DHCP client interfaces.

Z9500

Syntax

```
debug ip dhcp client packets [interface type slot/port]
```

Parameters**interface
typeslot/port**

Enter the keyword *interface* with the interface type and slot/port information to display DHCP log messages for a specified interface. The valid interface types are:

- For a 10-Gigabit Ethernet interface, enter the keyword *tengigabitethernet*.
- For a 40-Gigabit Ethernet interface, enter the keyword *fortyGigE*.

Defaults

none

**Command
Modes**

EXEC Privilege

**Command
History**

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```

Dell# debug ip dhcp client packets

Dell(conf)#do show debugging
Dhcp Client :
  DhcpClient Packet debugging is on for fortyGigE 2/0

Dell(conf-if-fo-2/0)#ip address dhcp
Dell(conf-if-fo-2/0)#no ip address dhcp

Dell(conf-if-fo-2/0)#do show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 5 Messages Logged, Size
(40960 bytes)
  Trap logging: level informational
    Logging to 10.10.10.4
    Logging to 10.1.2.4
    Logging to 172.31.1.4
    Logging to 133.33.33.4
    Logging to 172.16.1.162
  Last logging buffer cleared: Jan 7 01:41:17
Jan 7 01:42:34: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_PKT: DHCP RELEASE sent in Interface Fo 2/0
Jan 7 01:41:39: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_PKT: Received DHCPACK packet in InterfaceFo 2/0
with Lease-IP:100.1.1.253, Mask:255.255.255.0, Server-Id:
100.1.1.2
Jan 7 01:41:39: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_PKT: DHCP REQUEST sent in Interface Fo 2/0
Jan 7 01:41:36: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_PKT: Received DHCP OFFER packet in Interface Fo
2/0 with Lease-IP:100.1.1.253, Mask:255.255.255.0, Server-Id:

```

```

100.1.1.2
Jan 7 01:41:36: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG:
DHCLIENT_DBG_PKT: DHCP DISCOVER sent in Interface Fo 2/0

```

default-router

Assign a default gateway to clients based on the address pool.

Z9500

Syntax	<code>default-router address [address2...address8]</code>	
Parameters	address	Enter a list of routers that may be the default gateway for clients on the subnet. You may specify up to eight routers. List them in order of preference.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

disable

Disable the DHCP server.

Z9500

Syntax	<code>disable</code> DHCP Server is disabled by default. To enable the system to be a DHCP server, use the <code>no disable</code> command.
Defaults	Disabled
Command Modes	CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

dns-server

Assign a DNS server to clients based on address pool.

Z9500

Syntax

```
dns-server address [address2...address8]
```

Parameters

address	Enter a list of DNS servers that may service clients on the subnet. You may list up to eight servers, in order of preference.
----------------	---

Defaults

none

Command Modes

DHCP <POOL>

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

domain-name

Assign a domain to clients based on the address pool.

Z9500

Syntax	<code>domain-name name</code>	
Parameters	<i>name</i>	Give a name to the group of addresses in a pool.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

Z9500

Syntax	<code>excluded-address [address low-address high-address]</code>	
Parameters	<i>address</i>	Enter a single address to be excluded from the pool.
	<i>low-address</i>	Enter the lowest address in a range of addresses to be excluded from the pool.
	<i>high-address</i>	Enter the highest address in a range of addresses to be excluded from the pool.
Defaults	none	
Command Modes	DHCP	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

hardware-address

For manual configurations, specify the client hardware address.

Z9500

Syntax `hardware-address address`

Parameters

address	Enter the hardware address of the client.
----------------	---

Defaults none

Command Modes DHCP <POOL>

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

Z9500

Syntax	<code>host address</code>	
Parameters	<i>address/mask</i>	Enter the host IP address and subnet mask.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

ip address dhcp

Configure an interface to receive its IP address from the configured DHCP server.

Z9500

Syntax	<code>ip address dhcp</code> To release the IP address acquired from a DHCP server, enter the <code>no ip address dhcp</code> command.	
Defaults	Not configured.	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

You must be in INTERFACE mode in order to configure an interface to dynamically acquire an IP address from a DHCP server.

Use the `no ip address dhcp` in INTERFACE mode to:

- Release the IP address that was dynamically acquired from a DHCP server from the interface.
- Disable the DHCP client on the interface so it cannot acquire a dynamic IP address from a DHCP server.
- Stop DHCP packet transactions on the interface.

To release the IP address dynamically acquired from a DHCP server and allow an interface to acquire a new DHCP server-assigned address, enter the `release dhcp interface type slot/port` command in EXEC Privilege mode. To acquire a new server-assigned IP address, enter the `renew dhcp interface type slot/port` command in EXEC Privilege mode or the `ip address dhcp` command in INTERFACE Configuration mode.

ip address dhcp relay information-option

Include the relay-information option (option 81) in DHCP packets sent by the client. Some DHCP servers can be configured to allocate IP addresses based on option 81.

Z9500

Syntax

```
ip address dhcp relay information-option [remote-id [hostname |
mac | remote-id]
```

Parameters

remote-id hostname	Set the hostname as the remote ID in Option 82.
remote-id remote-id	Enter the name to be used as the remote ID in Option 82; maximum: 64 characters.
remote-id mac	Use the chassis MAC address as the remote ID in Option 82.

Default

Option 82 uses the chassis MAC address as the remote ID.

Command Modes	CONFIGURATION				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				
Usage Information	You can enter the <code>ip address dhcp relay information-option</code> and <code>ip address dhcp relay vendor-class-identifier</code> commands in the same <code>ip address dhcp</code> command line; for example: <pre>ip address dhcp vendor-class-identifier dell9500 relay information-option mac</pre> <pre>ip address dhcp relay information-option mac vendor-class- identifier dell9500</pre>				
Related Commands	ip address dhcp — configures an interface to receive its IP address from the configured DHCP server.				

ip address dhcp vendor-class-identifier

Include the vendor-class identifier option (option 60) in DHCP packets sent by the client.

Z9500

Syntax	ip address dhcp vendor-class-identifier text					
Parameters	vendor-class-identifier text	Include a user-configurable text string with the hardware-related information (option 60) in DHCP packets sent by the client (32 characters maximum).				
Default	None.					
Command Modes	CONFIGURATION					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					

**Usage
Information**

Use this command to include the vendor-class identifier (option 60) in DHCP packets sent by the client. This option is used by DHCP clients to identify the vendor type and configuration of a DHCP client. The vendor-class identifier includes hardware-related information that identifies the switch and includes a user-configurable text string .

You can enter the `ip address dhcp relay information-option` and `ip address dhcp relay vendor-class-identifier` commands in the same `ip address dhcp` command line; for example:

```
ip address dhcp vendor-class-identifier dell9500 relay
information-option mac
```

```
ip address dhcp relay information-option mac vendor-class-
identifier dell9500
```

**Related
Commands**

[ip address dhcp](#) — configures an interface to receive its IP address from the configured DHCP server.

lease

Specify a lease time for the addresses in a pool.

Z9500

Syntax

```
lease {days [hours] [minutes] | infinite}
```

Parameters

<i>days</i>	Enter the number of days of the lease. The range is from 0 to 31.
<i>hours</i>	Enter the number of hours of the lease. The range is from 0 to 23.
<i>minutes</i>	Enter the number of minutes of the lease. The range is from 0 to 59.
<i>infinite</i>	Specify that the lease never expires.

Defaults

24 hours

**Command
Modes**

DHCP <POOL>

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

netbios-name-server

Specify the NetBIOS Windows Internet Naming Service (WINS) name servers, in order of preference, that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

Z9500

Syntax	<code>netbios-name-server address [address2...address8]</code>	
Parameters	address	Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.
Defaults	none	
Command Modes	DHCP <POOL>	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as `hybrid`.

Z9500

Syntax	<code>netbios-node-type type</code>	
Parameters	type	Enter the NETBIOS node type: Broadcast: Enter the keyword <code>b-node</code>.

- Hybrid: Enter the keyword `h-node`.
- Mixed: Enter the keyword `m-node`.
- Peer-to-peer: Enter the keyword `p-node`.

Defaults	Hybrid												
Command Modes	DHCP <POOL>												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series and S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
8.2.1.0	Introduced on the C-Series and S-Series.												

network

Specify the range of addresses in an address pool.

Z9500

Syntax	<code>network network /prefix-length</code>									
Parameters	<i>network/ prefix-length</i>	Specify a range of addresses. Prefix-length range is from 17 to 31.								
Defaults	none									
Command Modes	DHCP <POOL>									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.3.19.0	Introduced on the S4820T.									
8.3.11.1	Introduced on the Z9000.									

Version	Description
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

pool

Create an address pool.

Z9500

Syntax	<code>pool name</code>	
Parameters	name	Enter the address pool's identifying name.
Defaults	none	
Command Modes	DHCP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp client statistics

Display statistical information about DHCP client interfaces.

Z9500

Syntax	<code>show ip dhcp client statistics [interface type slot/port]</code>	
Parameters	interface typeslot/port	Enter the keyword <code>interface</code> with the interface type and slot/port information to display DHCP client information for a specified interface. The valid interface types are: - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.

Defaults none

Command Modes EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp client statistics interface fortyGigE 2/0
Interface Name      Fo 2/0
Message             Received
DHCPPOFFER          9
DHCPACK              9
DHCPNAK              0
Message             Sent
DHCPDISCOVER        53
DHCPREQUEST         9
DHCPDECLINE          0
DHCPRELEASE         6
DHCPREBIND           0
DHCPRENEW            0
DHCPINFORM           0
```

show ip dhcp configuration

Display the DHCP configuration.

Z9500

Syntax show ip dhcp configuration [global | pool *name*]

Parameters

pool <i>name</i>	Display the configuration for a DHCP pool.
global	Display the DHCP configuration for the entire system.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp configuration global

Protocol status      : Enabled
Number of ping packets : 1
Dell#

Dell# show ip dhcp configuration pool p1

Pool Name           : p1
Pool Type           : Dynamic
Domain Name         : dell.com
Lease Time          : 2Days 0Hrs 0Mins
DNS Servers         : 10.11.0.1
Default Routers     : 1.1.1.1
Network             : 1.1.1.0 255.255.255.0
```

show ip dhcp conflict

Display the address conflict log.

Z9500

Syntax `show ip dhcp conflict address`

Parameters

address	Display a particular conflict log entry.
----------------	--

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp lease

Display lease information about the dynamic IP address currently assigned to a DHCP client interface.

Z9500

Syntax	<code>show ip dhcp dhcp lease [interface type slot/port]</code>	
Parameters	interface type slot/port	Enter the keyword <code>interface</code> with the interface type and slot/port information to display DHCP lease information for a specified interface. The valid interface types are: - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp server statistics

Display statistical information about a DHCP server.

Z9500

Syntax	<code>show ip dhcp server statistics</code>
Defaults	none
Command Modes	EXEC Privilege

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on the C-Series and S-Series.

Example

```

Dell# show ip dhcp server statistics
Address pools          1
Database agents        0
Automatic bindings     10
Manual bindings        0
Expired bindings       1
Malformed messages     0

Message                Received
BOOTREQUEST            0
DHCPDISCOVER           10
DHCPREQUEST            16
DHCPDECLINE            0
DHCPRELEASE            8
DHCPINFORM             0

Message                Sent
BOOTREPLY              0
DHCPOFFER              10
DHCPACK                16
DHCPNAK                0

```

Configure Secure DHCP and DHCP Relay

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks, including using the switch as a DHCP relay agent.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

Z9500

Syntax	<code>arp inspection</code>
Defaults	Disabled
Command Modes	INTERFACE VLAN
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands [arp inspection-trust](#) — specifies a port as trusted so that ARP frames are not validated against the binding table.

arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

Z9500

Syntax `arp inspection-trust`

Defaults Disabled

Command Modes

- INTERFACE
- INTERFACE PORT-CHANNEL

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands [arp inspection](#) — enables dynamic ARP inspection on a VLAN.

clear ip dhcp snooping

Clear the DHCP binding table.

Z9500

Syntax `clear ip dhcp snooping binding`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.

ip dhcp snooping

Enable DHCP snooping globally.

Z9500

Syntax `[no] ip dhcp snooping`

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.2.(0.0)	Introduced on the S4810 and S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series on Layer 2 interfaces.
7.8.1.0	Introduced on the C-Series and S-Series on Layer 3 interfaces.

Usage Information

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table deletes and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

DHCP snooping supports Layer 3 using DHCP Relay Agent (`ip helper-address`) and Layer 2. You do not have to enable relay agent to snoop on Layer 2 interfaces.

Related Commands

[ip dhcp snooping vlan](#) — enables DHCP snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Z9500

Syntax

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number
```

Parameters

mac address	Enter the keyword <code>mac</code> then the MAC address of the host to which the server is leasing the IP address.
vlan-id vlan-id	Enter the keywords <code>vlan-id</code> then the VLAN to which the host belongs. The range is from 2 to 4094.
ip ip-address	Enter the keyword <code>ip</code> then the IP address that the server is leasing.
interface type	Enter the keyword <code>interface</code> then the type of interface to which the host is connected: - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
slot/port	Enter the slot and port number of the interface.
lease time	Enter the keyword <code>lease</code> then the amount of time the IP address are leased. The range is from 1 to 4294967295.

Defaults	none																
Command Modes	- EXEC - EXEC Privilege																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.1.0</td><td>Introduced on the E-Series.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Introduced on the E-Series.	7.8.1.0	Introduced on the C-Series and S-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																
8.3.7.0	Introduced on the S4810.																
8.3.1.0	Introduced on the E-Series.																
7.8.1.0	Introduced on the C-Series and S-Series.																
Related Commands	show ip dhcp snooping — displays the contents of the DHCP binding table.																

ip dhcp snooping database

Delay writing the binding table for a specified time.

Z9500

Syntax	ip dhcp snooping database write-delay <i>minutes</i>							
Parameters	<i>minutes</i>	The range is from 5 to 21600.						
Defaults	none							
Command Modes	CONFIGURATION							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping database renew

Renew the binding table.

Z9500

Syntax `ip dhcp snooping database renew`

Defaults `none`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping trust

Configure an interface as trusted.

Z9500

Syntax `[no] ip dhcp snooping trust`

Defaults **Untrusted**

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping verify mac-address

Validate a DHCP packet's source hardware address against the client hardware address field (CHADDR) in the payload.

Z9500

Syntax [no] ip dhcp snooping verify mac-address

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.2.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

Z9500

Syntax	[no] ip dhcp snooping vlan <i>name</i>											
Parameters	<i>name</i>	Enter the name of a VLAN on which to enable DHCP Snooping.										
Defaults	Disabled											
Command Modes	CONFIGURATION											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.1.0</td><td>Introduced on the E-Series.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.3.1.0	Introduced on the E-Series.	7.8.1.0	Introduced on the C-Series and S-Series.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.11.1	Introduced on the Z9000.											
8.3.1.0	Introduced on the E-Series.											
7.8.1.0	Introduced on the C-Series and S-Series.											
Usage Information	When enabled, the system begins creating entries in the binding table for the specified VLANs.  NOTE: Learning only happens if there is a trusted port in the VLAN.											
Related Commands	ip dhcp snooping trust — configures an interface as trusted.											

ip dhcp source-address-validation

Enable the IP Source Guard.

Z9500

Syntax	[no] ip dhcp source-address-validation [ipmac]	
Parameters	ipmac	Enable IP+MAC Source Address Validation.
Defaults	Disabled	
Command Modes	INTERFACE	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Added the keyword <code>ipmac</code> .
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

Allocate at least one FP block to `ipmacacl` before you can enable IP+MAC Source Address Validation.

1. Use the `cam-acl 12acl` command from CONFIGURATION mode.
2. Save the running-config to the startup-config.
3. Reload the system.

show ip dhcp binding

Display the DHCP binding table.

Z9500

Syntax	<code>show ip dhcp binding</code>
Defaults	none
Command Modes	EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
1.1.1.253	00:00:00:00:00:10	Jan 08 2014 23:57	
Automatic			
1.1.1.254	00:00:00:00:00:20	Jan 08 2014 23:57	
Automatic			

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

Z9500

Syntax `show ip dhcp snooping [binding | source-address-validation]`

Parameters

binding	Display the interfaces configured with IP Source Guard.
source-address-validation	Display the interfaces configured with IP Source Guard.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands

[clear ip dhcp snooping](#) — clears the contents of the DHCP binding table.

Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) supports multiple "best paths" in next-hop packet forwarding to a destination device.

ecmp-group

Provides a mechanism to monitor traffic distribution on an ECMP link bundle. A system log is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

Z9500

Syntax

```
ecmp-group {ecmp-group-id interface interface | link-bundle-monitor}
```

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

Parameters

- | | |
|-----------------------------|---|
| <i>ecmp-group ID</i> | Enter the identifier number for the ECMP group. The range is from 2 to 64. |
| <i>interface</i> | <p>Enter the following keywords and slot/port to add the interface to the ECMP group:</p> <ul style="list-style-type: none"> • 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information • For a LAG interface, enter the keywords <code>port-channel</code> then the slot/port information. The range is from 1 to 128. |

Defaults

Off

Command Modes

- CONFIGURATION
- CONFIGURATION ECMP-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

Usage Information	Using CONFIGURATION mode, create an ECMP group ID. You can then assign interfaces to the ECMP group using CONFIGURATION ECMP-GROUP mode. You can also enable on the port-channel configuration using the CONFIGURATION ECMP-GROUP command mode.
--------------------------	---

hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a port channel.

Z9500

Syntax

```
hash-algorithm {ecmp {crc16 | crc16cc | crc32MSB | crc32LSB |
crc-upper | dest-ip | lsb | xor1 | xor2 | xor4 | xor8 | xor16}
hg {crc16 | crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4
| xor8 | xor16} {hg-seed seed-value} lag {crc16 | crc16cc |
crc32MSB | crc32LSB | xor1 | xor2 | xor4 | xor8 | xor16} | seed
seed-value} linecard slot-id | port-set port-pipe
```

To return to the default hash algorithm, use the `no hash-algorithm` command.

To return to the default ECMP hash algorithm, use the `no hash-algorithm ecmp algorithm-value` command.

To remove the hash algorithm on a particular line card, use the `no hash-algorithm linecard number` command.

Parameters

ecmp <i>crc16</i> <i>crc16cc</i> <i>crc32MSB</i> <i>crc32LSB</i> <i>crc-upper</i> <i>dest-ip</i> <i>lsb</i> <i>xor1</i> <i>xor2</i> <i>xor4</i> <i>xor8</i> <i>xor16</i>	Enter the keyword <code>ecmp</code> then one of the following options: <i>crc16</i>: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default) <i>crc16cc</i>: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial <i>crc32MSB</i>: Use CRC32_UPPER — MSB 16 bits of computed CRC32 <i>crc32LSB</i>: Use CRC32_LOWER — LSB 16 bits of computed CRC32 <i>crc-upper</i>: Uses the upper 32 bits of the key for the hash computation
---	---

- *dest-ip*: Uses the destination IP for ECMP hashing
- *lsb*: Returns the LSB of the key as the hash
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16 bit XOR

**hg {crc16 |
crc16cc |
crc32MSB |
crc32LSB | xor1
| xor2 | xor4 |
xor8 | xor16}**

Enter the keyword **hg** then one of the following options:

- *crc16*: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16 bit XOR

**hg-seed seed-
value**

Enter the keywords **hg-seed** then the hash algorithm seed value. The range is from 0 to 2147483646.

**lag {crc16 |
crc16cc |
crc32MSB |
crc32LSB | xor1
| xor2 | xor4 |
xor8 | xor16}**

Enter the keyword **lag** then one of the following options:

- *crc16*: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4

	• <code>xor8</code>: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8 • <code>xor16</code>: Use CR16 — 16 bit XOR
seed seed-value	Enter the keyword <code>seed</code> then the hash algorithm seed value. The range is from 0 to 2147483646.
linecard slot-id port-set port-pipe	Enter the <code>linecard slot-id</code> parameters to specify a Z9500 line card. The slot IDs range from 0 to 2. Enter the <code>port-set port-pipe</code> parameters to specify a port pipe (set of ports) on the line card. The port-pipe range is from 0 to 3.

Defaults IPSA and IPDA mask value is **FF** for the line card.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Added the <code>nh-ecmp</code> option.
7.7.1.1	Added the <code>nh-ecmp</code> option.
6.5.1.0	Added the <code>line card</code> option on TeraScale only.
6.3.1.0	Added support for ECMP and LAG on TeraScale only.

Usage Information To ensure that CRC is not used for LAG, set the default hash-algorithm method. For example, `hash-algorithm ecmp xor lag checksum nh-ecmp checksum`.

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.

The line-card option is applicable with the lag-hash-align microcode only. Any other microcode returns an error message as follows:

- `Dell(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff`
- `% Error: This command is not supported in the current microcode configuration`

In addition, the `linecard slot-id ip-sa-mask value ip-da-mask value` option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the `ip-sa-mask` and `ip-da-mask` values must be equal. (Single Linecard).
- When hashing is done only on IPSA or IPDA, the system maintains bi-directionality with masks set to `XX 00` for line card 1 and `00 XX` for line card 2 (`ip-sa-mask` and `ip-da-mask`). The mask value must be the same for both line cards when using multiple line cards as ingress (where `XX` is any value from `00` to `FF` for both line cards). For example, assume that traffic is flowing between line card 1 and line card 2:
 - `hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00`
 - `hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa`

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, use the `hash-algorithm` command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

Z9500

Term heading	Description heading				
Syntax	<pre>hash-algorithm ecmp {crc-upper} {dest-ip} {lsb}</pre> To return to the default hash algorithm, use the <code>no hash-algorithm ecmp</code> command.				
Parameters	<table> <tr> <td>crc-upper</td><td>Uses the upper 32 bits of the key for the hash computation. The default is crc-lower.</td></tr> <tr> <td>dest-ip</td><td>Uses the destination IP for ECMP hashing. The default is enabled.</td></tr> </table>	crc-upper	Uses the upper 32 bits of the key for the hash computation. The default is crc-lower .	dest-ip	Uses the destination IP for ECMP hashing. The default is enabled .
crc-upper	Uses the upper 32 bits of the key for the hash computation. The default is crc-lower .				
dest-ip	Uses the destination IP for ECMP hashing. The default is enabled .				

Term heading	Description heading lsb Returns the LSB of the key as the hash. The default is crc-lower.																
Defaults	• crc-lower • dest-ip enabled																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.1.1.0	Introduced on the E-Series ExaScale.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
Usage Information	The hash value calculated with the <code>hash-algorithm</code> command is unique to the entire chassis. The default ECMP hash configuration is crc-lower. This command takes the lower 32 bits of the hash key to compute the egress port and is the "fall-back" configuration if you have not configured anything else. The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, use this command to designate another algorithm. When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.																

hash-algorithm hg

To distribute traffic flows across different internal HiGig links, change the hash algorithm.

Z9500

Syntax hash-algorithm hg {*crc16* | *xor1* | *xor2* | *xor4* | *xor8* | *xor16* | *crc16cc* | *crc32MSB* | *crc32LSB*} linecard *slot-id* port-set *port-pipe*

Parameters	<i>crc16</i>	Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default).
	<i>xor1</i>	Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1.
	<i>xor2</i>	Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2.
	<i>xor4</i>	Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4.
	<i>xor8</i>	Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8.
	<i>xor16</i>	Use CR16 — 16 bit XOR.
	<i>crc16cc</i>	Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial.
	<i>crc32MSB</i>	Use CRC32_UPPER — MSB 16 bits of computed CRC32.
	<i>crc32LSB</i>	Use CRC32_LOWER — LSB 16 bits of computed CRC32.
	linecard <i>slot-id</i> port-set <i>port-pipe</i>	Enter the line-card slot ID and port-pipe number for the set of ports for which you want to redistribute traffic flows. The range of Z9500 slot IDs is 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.

Defaults **crc16 algorithm**
Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.
The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.4	Introduced on the Z9000.

hash-algorithm hg-seed

Select the seed value used in HiGig hashing.

Z9500

Syntax	<code>[no] hash-algorithm hg-seed <i>number</i> [linecard <i>slot-id</i> port-set <i>port-pipe</i>]</code>	
Parameters	hg-seed <i>number</i>	Enter the keywords <code>hg-seed</code> then the hash algorithm seed value. The range is from 0 to 2147483646.
	linecard <i>slot-id</i> port-set <i>port-pipe</i>	(Optional) Enter the line-card slot ID and port-pipe number for the set of ports for which you configure HiGig hashing. The range of Z9500 slot IDs is 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.
Defaults	32-bit chassis MAC and system time	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.4	Introduced on the Z9000.

hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

Z9500

Syntax	<code>hash-algorithm seed <i>value</i> [linecard <i>slot</i>] [port-set <i>number</i>]</code>	
Parameters	seed <i>value</i>	Enter the keyword <code>seed</code> then the seed value. The range is from 0 to 4095.
	linecard <i>slot</i>	Enter the keyword <code>linecard</code> then the linecard slot number.
	port-set <i>number</i>	Enter the keyword <code>port-set</code> then the linecard port-pipe number.

Defaults	none												
Command Modes	CONFIGURATION												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Introduced on the E-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
8.3.1.0	Introduced on the E-Series.												
Usage Information	Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This behavior means that for a given flow, even though the prefixes are sorted, two unrelated chassis select different hops. The system provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.  NOTE: While the seed is stored separately on each port-pipe, the same seed is used across all CAMs. You cannot separate LAG and ECMP but you can use different algorithms across the chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior. If the hash algorithm configuration is removed, the hash seed does not go to the original factory default setting.												

ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM hold for a route, By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

Z9500

Syntax `ip ecmp-group {maximum-paths | {number} {path-fallback}`

To negate a command, use the `no ip ecmp-group maximum-paths {number}` command.

Parameters	maximum-paths	Specify the maximum number of ECMP for a route. The range is 2 to 64.
	path-fallback	Use the keywords <code>path-fallback</code> to enable this feature. If you enable the feature, re-enter this keyword to disable the feature.
Defaults	16	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	9.0.0.0	Introduced on the Z9000.
	8.3.10.0	Introduced on the S4810.
Usage Information	You must save the new ECMP settings to the startup-config (<code>write mem</code>) then reload the system for the new settings to take effect.	
Related Commands	show ip cam linecard – Display content-addressable memory (CAM) entries for a set of ports on a line card.	

link-bundle-distribution trigger-threshold

Provides a mechanism to set the threshold to trigger when traffic distribution begins being monitored on an ECMP link bundle.

Z9500

Syntax	<code>link-bundle-distribution trigger-threshold [percent]</code>	
	To exit from <code>ecmp group</code> mode, use the <code>exit</code> command.	
Parameters	percent	Indicate the threshold value when traffic distribution starts being monitored on an ECMP link bundle. The range is from 1 to 90%. The default is 60% .
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

link-bundle-monitor enable

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

Z9500

Syntax `link-bundle-monitor enable`
To exit from ECMP group mode, use the `exit` command.

Command Modes

- ECMP-GROUP
- PORT-CHANNEL INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

show config

Display the ECMP configuration.

Z9500

Syntax `show config`

Command Modes	CONFIGURATION-ECMP-GROUP										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										
Related Commands	show running-config ecmp-group — displays interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution.										

show link-bundle distribution

Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

Z9500

Syntax	<code>show link-bundle-distribution</code>										
Command Modes	EXEC Privilege										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										
Example	<pre>Dell#show link-bundle-distribution Link-bundle trigger threshold - 60 ECMP bundle - 5 Utilization[In Percent] - 0 Alarm State - Inactive Interface Line Protocol Utilization[In Percent]</pre>										

Te 0/4	Up	5
Te 0/3	Up	30

FIPS Cryptography

To configure federal information processing standards (FIPS) cryptography, use the commands described in this chapter.

fips mode enable

Enable the FIPS cryptography mode on the platform.

Z9500

Syntax	<code>[no] fips mode enable</code> To disable the FIPS cryptography mode, use the <code>no fips mode enable</code> command.										
Default	Disabled										
Command Modes	CONFIGURATION										
Example	<pre>Dell(conf)#fips mode enable WARNING: Enabling FIPS mode will close all SSH/Telnet connection, restart those servers, and destroy all configured host keys. proceed (y/n) ? y Dell(conf)#</pre>										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </tbody> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.1(0.0)	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description										
9.5(0.1)	Introduced on the Z9500.										
9.1(0.0)	Introduced on the Z9000.										
8.3.19.0	Introduced on the S4820T.										
8.3.12.0	Introduced on the S4810.										

show fips status

Displays the status of the FIPS mode.

Z9500

Syntax `show fips status`

Defaults None

Command Modes EXEC

Example

```
Dell#show fips status
FIPS Mode: Enabled
Dell#
```

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

show ip ssh

Display information about established SSH sessions

Z9500

Syntax `show ip ssh`

Defaults none

Command Modes EXEC
EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell #show ip ssh
SSH server : enabled.
SSH server version : v1 and v2.
Password Authentication : enabled.
Hostbased Authentication : disabled.
RSA Authentication : disabled.
Vty Encryption HMAC Remote IP
1 3des-cbc hmac-md5 10.1.20.48
2 3des-cbc hmac-md5 10.1.20.48
```

With FIPS Mode enabled:

```
Dell #show ip ssh
SSH server : enabled.
SSH server version : v2.
Password Authentication : enabled.
Hostbased Authentication : disabled.
RSA Authentication : disabled.
Vty Encryption HMAC Remote IP
0 aes128-cbc hmac-sha1 10.11.8.13
1 aes128-cbc hmac-sha1 10.1.20.48
```

ssh

Open an SSH connection specifying the hostname, username, port number, and version of the SSH client.

Z9500

Syntax

```
ssh {hostname|ipv4 address|ipv6 address} [-c encryption cipher|-l username|-m HMAC algorithm|-p port-number|-v {1|2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6 addressprefix	(OPTIONAL) Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

-c encryption cipher	Enter the following encryption cipher to use. (For v2 clients only.) Without the FIPS mode enabled: • 3des-cbc: Force ssh to use 3des-cbc encryption cipher. With the FIPS mode enabled: • aes128-cbc: Force ssh to use the aes128-cbc encryption cipher. • aes256-cbc: Force ssh to use the aes256-cbc encryption cipher.
-l username	(OPTIONAL) Enter the keyword <code>-l</code> then the user name used in this SSH session. The default is the user name of the user associated with the terminal.
-m HMAC algorithm	Enter one of the following HMAC algorithms to use. (For v2 clients only.): Without the FIPS mode enabled: • hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm. • hmac-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm. • hmac-md5: Force ssh to use the hmac-md5 HMAC algorithm. • hmac-md5-96: Force ssh to use the hmac-md5-96 HMAC algorithm. With the FIPS mode enabled: • hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm. • hmac-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm.
-p port-number	(OPTIONAL) Enter the keyword <code>-p</code> then the port number. The range is 1 to 65536 The default is 22
-v {1 2}	(OPTIONAL) Enter the keyword <code>-v</code> then the SSH version 1 or 2. The default: The version from the protocol negotiation.
	 NOTE: If the FIPS mode is enabled, this option does not display in the output.

Defaults

As indicated above.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Related Commands

ip ssh server	Configure an SSH server.
show ip ssh client-pub-keys	Display the client-public keys.

Usage Information

Both inbound and outbound SSH sessions using IPv4 or IPv6 addressing are supported. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

Example**If FIPS mode is not enabled:**

```
Dell#ssh 10.11.8.12 ?
-c      Encryption cipher to use (for v2 client
-l      User name option
-m      HMAC algorithm to use (for v2 clients only)
-p      SSH server port option (default 22)
-v      SSH protocol version
<cr>
Dell#ssh 10.11.8.12 -c ?
3des-cbc      Force ssh to use 3des-cbc encryption cipher
Dell #ssh 10.11.8.12 -m ?
hmac-sha1     Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96  Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5      Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96   Force ssh to use hmac-md5-96 HMAC algorithm
```

With FIPS mode enabled:

```
Dell#ssh 10.11.8.12 ?
-c      Encryption cipher to use (for v2 client
-l      User name option
-m      HMAC algorithm to use (for v2 clients only)
-p      SSH server port option (default 22)
<cr>
Dell#ssh 10.11.8.12 -c ?
```

```
aes128-cbc      Force ssh to use aes128-cbc encryption cipher
aes256-cbc      Force ssh to use aes256-cbc encryption cipher
Dell #ssh 10.11.8.12 -m ?
hmac-sha1       Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96    Force ssh to use hmac-sha1-96 HMAC algorithm
```

Force10 Resilient Ring Protocol (FRRP)

Force10 resilient ring protocol (FRRP) is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the spanning tree protocol (STP).

The resilient ring protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as the control VLAN for a ring cannot be configured as a control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

clear frrp

Clear the FRRP statistics counters.

Z9500

Syntax	<code>clear frrp [ring-id]</code>	
Parameters	ring-id	(Optional) Enter the ring identification number. The range is from 1 to 255.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series.	7.5.1.0	Introduced.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.2.1.0	Introduced on the C-Series.														
7.5.1.0	Introduced.														
Usage Information	Executing this command without the optional <code>ring-id</code> command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters: • hello Rx and Tx counters • Topology change Rx and Tx counters • The number of state change counters														
Example	<pre>Dell#clear frrp Clear frrp statistics counter on all ring [confirm] yes Dell#clear frrp 4 Clear frrp statistics counter for ring 4 [confirm] yes Dell#</pre>														
Related Commands	show frrp — displays the Resilient Ring Protocol configuration.														

debug frrp

Clear the FRRP statistics counters.

Z9500

Syntax	<pre>debug frrp {event packet detail} [<i>ring-id</i>] [count <i>number</i>]</pre> To disable debugging, use the <code>no debug frrp {event packet detail} [<i>ring-id</i>] [countnumber]</code> command.	
Parameters	event	Enter the keyword <code>event</code> to display debug information related to ring protocol transitions.
	packet	Enter the keyword <code>packet</code> to display brief debug information related to control packets.

	detail	Enter the keyword <code>detail</code> to display detailed debug information related to the entire ring protocol packets.																
	ring-id	(Optional) Enter the ring identification number. The range is from 1 to 255.																
	count <i>number</i>	Enter the keyword <code>count</code> then the number of debug outputs. The range is from 1 to 65534.																
Defaults	Disabled.																	
Command Modes	CONFIGURATION (conf-frpp)																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series.	7.4.1.0	Introduced.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
8.2.1.0	Introduced on the C-Series.																	
7.4.1.0	Introduced.																	
Usage Information	Because the resilient ring protocol can potentially transmit 20 packets per interface, restrict debug information.																	

description

Enter an identifying description of the ring.

Z9500

Syntax	<code>description Word</code> To remove the ring description, use the <code>no description [Word]</code> command.	
Parameters	Word	Enter a description of the ring. Maximum: 255 characters.
Defaults	none	

Command Modes

CONFIGURATION (conf-frp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

disable

Disable the resilient ring protocol.

Z9500

Syntax

`disable`

To enable the Resilient Ring Protocol, use the `no disable` command.

Defaults

Disabled

Command Modes

CONFIGURATION (conf-frp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

interface

Configure the primary, secondary, and control-vlan interfaces.

Z9500

Syntax `interface {primary interface secondary interface control-vlan vlan-id}`

To return to the default, use the `no interface {primary interface secondary interface control-vlan vlan-id}` command.

Parameters

primary <i>interface</i>	Enter the keyword <code>primary</code> to configure the primary interface then one of the following interfaces and slot/port information: - Fast Ethernet interface: enter the keyword <code>FastEthernet</code> then the slot/port information. - Port Channel interface: enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. 10-Gigabit Ethernet interface: enter the keyword <code>TenGigabitEthernet</code> then the slot/port information 40-Gigabit Ethernet interface: enter the keyword <code>fortyGigE</code> then the slot/port information
secondary <i>interface</i>	Enter the keyword <code>secondary</code> to configure the secondary interface then one of the following interfaces and slot/port information: - Fast Ethernet interface: enter the keyword <code>FastEthernet</code> then the slot/port information. - Port Channel interface: enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. 10-Gigabit Ethernet interface: enter the keyword <code>TenGigabitEthernet</code> then the slot/port information 40-Gigabit Ethernet interface: enter the keyword <code>fortyGigE</code> then the slot/port information
control-vlan <i>vlan-id</i>	Enter the keyword <code>control-vlan</code> then the VLAN ID. The range is from 1 to 4094.

Defaults	none																
Command Modes	CONFIGURATION (conf-frrp)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series.	7.4.1.0	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.11.1	Introduced on the Z9000.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.2.1.0	Introduced on the C-Series.																
7.4.1.0	Introduced.																
Usage Information	This command causes the Ring Manager to take ownership of the two ports after IFM validates the configuration. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.																
Related Commands	show frrp — displays the Resilient Ring Protocol configuration information.																

member-vlan

Specify the member VLAN identification numbers.

Z9500

Syntax	<pre>member-vlan {vlan-range}</pre> To return to the default, use the <code>no member-vlan [vlan-range]</code> command.	
Parameters	<i>vlan-range</i>	Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10. Combination: 3, 4, 5-10, 8.
Defaults	none	

Command Modes	CONFIGURATION (conf-frp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

mode

Set the Master or Transit mode of the ring.

Z9500

Syntax	<pre>mode {master transit}</pre> To reset the mode, use the <code>no mode {master transit}</code> command.	
Parameters	master	Enter the keyword <code>master</code> to set the Ring node to Master mode.
	transit	Enter the keyword <code>transit</code> to set the Ring node to Transit mode.

Defaults	Mode None
Command Modes	CONFIGURATION (conf-frp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

protocol frrp

Enter the Resilient Ring Protocol and designate a ring identification.

Z9500

Syntax `protocol frrp {ring-id}`
 To exit the ring protocol, use the `no protocol frrp {ring-id}` command.

Parameters *ring-id* Enter the ring identification number. The range is from 1 to 255.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information This command places you into the resilient ring protocol. After executing this command, the command line prompt changes to `conf-frrp`.

show frrp

Display the resilient ring protocol configuration.

Z9500

Syntax	show frrp [ring-id [summary]] [summary]															
Parameters	ring-id	Enter the ring identification number. The range is from 1 to 255														
	summary	(OPTIONAL) Enter the keyword summary to view just a summarized version of the Ring configuration.														
Defaults	none															
Command Modes	EXEC															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series.	7.4.1.0	Introduced.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
8.2.1.0	Introduced on the C-Series.															
7.4.1.0	Introduced.															
Usage Information	Executing this command without the optional ring-id command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters: • hello Rx and Tx counters • Topology change Rx and Tx counters • The number of state change counters															
Usage Information	Executing this command without the optional ring-id command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command is executed. This command clears the following counters: • hello Rx and Tx counters • Topology change Rx and Tx counters															

- The number of state change counters

Example (Summary)

```
Dell#show frrp summary
Ring-ID State Mode Ctrl_Vlan Member_Vlans
-----
2        UP   Master  2        11-20, 25,27-30
31       UP   Transit 31       40-41
50       Down Transit 50       32
Dell#
```

Example (1)

```
Dell#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : TenGigabitEthernet 0/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009
Dell#
```

Example (2 Summary)

```
Dell#show frrp 2 summary
Dell#show frrp 2 summary
Ring-ID State Mode Ctrl_Vlan Member_Vlans
-----
2        Up    Master  2        11-20, 25, 27-30
Dell#
```

Related Commands

[protocol frrp](#) — enters the resilient ring protocol and designate a ring identification.

timer

Set the hello interval or dead interval for the Ring control packets.

Z9500

Syntax

```
timer {hello-interval milliseconds}| {dead-interval
milliseconds}
```

To remove the timer, use the `no timer {hello-interval [milliseconds]}| {dead-interval milliseconds}` command.

Parameters

hello-interval
milliseconds

Enter the keyword `hello-interval` then the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 millisecond; for example, 50, 100, 150, and so on. If an

invalid value is entered, an error message is generated. The range is from 50 to 2000 ms. Default: **500 ms**.

**dead-interval
milliseconds**

Enter the keyword `dead-interval` then the time, in milliseconds, to set the dead interval of the control packets. The range is from 50 to 6000 ms. Default: **1500 ms**.



NOTE: The configured dead interval must be at least three times the hello interval.

Defaults

- **500 ms** for `hello-interval milliseconds`
- **1500 ms** for `dead-interval milliseconds`

Command Modes

CONFIGURATION (conf-frp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information

The `hello interval` command is the interval at which ring frames are generated from the primary interface of the master node. The `dead interval` command is the time that elapses before a time-out occurs.

GARP VLAN Registration (GVRP)

The Dell Networking OS supports basic GVRP commands on the switch.

The generic attribute registration protocol (GARP) mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

- The GVRP application
- GARP information propagation (GIP)
- GARP information declaration (GID)

Important Points to Remember

- GVRP is supported on Layer 2 ports only.
- All VLAN ports added by GVRP are tagged.
- GVRP is supported on untagged ports belonging to a default VLAN and tagged ports.
- GVRP cannot be enabled on untagged ports belonging to a non-default VLAN *unless* native VLAN is turned on.
- GVRP requires end stations with dynamic access NICs.
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If you enable GVRP, a port that changes to the STP Forwarding state automatically begin to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.

- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge must classify and analyze packets by VLAN protocols, manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge must know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

clear gvrp statistics

Clear GVRP statistics on an interface.

Z9500

Syntax	<code>clear gvrp statistics interface <i>interface</i></code>	
Parameters	interface	Enter the following keywords and slot/port or number information:
	<i>interface</i>	• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands [show gvrp statistics](#) — displays the GVRP statistics.

debug gvrp

Enable debugging on GVRP.

Z9500

Syntax `debug gvrp {config | events | pdu}`
To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

Parameters	config	Enter the keyword <code>config</code> to enable debugging on the GVRP configuration.
	event	Enter the keyword <code>event</code> to enable debugging on the JOIN/LEAVE events.
	pdu	Enter the keyword <code>pdu</code> then one of the following Interface keywords and slot/port or number information:
		- For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

Defaults Disabled.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

disable

Globally disable GVRP.

Z9500

Syntax	<pre>disable</pre> To re-enable GVRP, use the <code>no disable</code> command.												
Defaults	Enabled.												
Command Modes	CONFIGURATION-GVRP												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on C-Series, E-Series, and S-Series</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on C-Series, E-Series, and S-Series
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
7.6.1.0	Introduced on C-Series, E-Series, and S-Series												
Related Commands	gvrp enable — enables GVRP on physical interfaces and LAGs. protocol gvrp — access GVRP protocol.												

garp timers

Set the intervals (in milliseconds) for sending GARP messages.

Z9500

Syntax	<pre>garp timers {join leave leave-all}</pre>
---------------	---

To return to the previous setting, use the `no garp timers {join | leave | leave-all}` command.

Parameters

join Enter the keyword `join` then the number of milliseconds to configure the join time. The range is from 100 to 147483647 milliseconds. The default is **200 milliseconds**.



NOTE: Designate the milliseconds in multiples of 100.

leave Enter the keyword `leave` then the number of milliseconds to configure the leave time. The range is from 100 to 2147483647 milliseconds. The default is **600 milliseconds**.



NOTE: Designate the milliseconds in multiples of 100.

leave-all Enter the keywords `leave-all` then the number of milliseconds to configure the leave-all time. The range is from 100 to 2147483647 milliseconds. The default is 1000 milliseconds.



NOTE: Designate the milliseconds in multiples of 100.

Defaults

As above.

Command Modes

CONFIGURATION-GVRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information

- **Join Timer** — `Join` messages announce the willingness to register some attributes with other participants. For reliability, each GARP application entity sends a `Join` message twice and uses a join timer to set the sending interval.
- **Leave Timer** — `Leave` announces the willingness to de-register with other participants. Together with `Join`, `Leave` messages help GARP participants complete attribute reregistration and de-registration. The leave timer starts after receipt of a leave message sent for de-registering some attribute information. If a `Join` message is *not* received before the `Leave` time expires, the GARP application entity removes the attribute information as requested.

- **Leave All Timer** — The `Leave All` timer starts when a GARP application entity starts. When this timer expires, the entity sends a `Leave-all` message so that other entities can reregister their attribute information. Then the `Leave-all` time begins again.

**Related
Commands**

[show garp timers](#) — displays the current GARP times.

gvrp enable

Enable GVRP on physical interfaces and LAGs.

Z9500

Syntax

`gvrp enable`

To disable GVRP on the interface, use the `no gvrp enable` command.

Defaults

Disabled.

**Command
Modes**

CONFIGURATION-INTERFACE

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

**Related
Commands**

[disable](#) — globally disables GVRP.

gvrp registration

Configure the GVRP register type.

Z9500

Syntax

Related
Commands

[show gvrp](#) — displays the GVRP configuration including the registration.

protocol gvrp

Access GVRP protocol — (config-gvrp)#.

Z9500

Syntax `protocol gvrp`

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related
Commands

[disable](#) — globally disables GVRP.

show config

Display the global GVRP configuration.

Z9500

Syntax `show config`

Command Modes CONFIGURATION-GVRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

**Related
Commands**

[gvrp enable](#) — enables GVRP on physical interfaces and LAGs.

[protocol gvrp](#) — accesses the GVRP protocol.

show garp timers

Display the GARP timer settings for sending GARP messages.

Z9500

Syntax `show garp timers`

Defaults `none`

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History** This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Example

```
Dell#show garp timers
GARP Timers      Value (milliseconds)
-----
Join Timer       200
Leave Timer       600
```

```
LeaveAll Timer      10000
Dell#
```

Related Commands [garp timers](#) — sets the intervals (in milliseconds) for sending GARP messages.

show gvrp

Display the GVRP configuration.

Z9500

Syntax `show gvrp [brief | interface]`

Parameters

brief	(OPTIONAL) Enter the keyword <code>brief</code> to display a brief summary of the GVRP configuration.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information	If no ports are GVRP participants, the message output changes from GVRP Participants running on <port_list> to GVRP Participants running on no ports.
Example	<pre>R3#show gvrp brief GVRP Feature is currently enabled. Port GVRP Status Edge-Port ----- Te 1/0 Disabled No Te 1/1 Disabled No Te 1/2 Enabled No Te 1/3 Disabled No Te 1/4 Disabled No Te 1/5 Disabled No Te 1/6 Disabled No Te 1/7 Disabled No Te 1/8 Disabled No R3#show gvrp brief</pre>
Related Commands	show gvrp statistics — displays the GVRP statistics.

show gvrp statistics

Display the GVRP configuration statistics.

Z9500

Syntax	<code>show gvrp statistics {interface interface summary}</code>	
Parameters	interface <i>interface</i> (OPTIONAL) Enter the keyword <code>interface</code> then one of the interface keywords and slot/ port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.	
	summary Enter the keyword <code>summary</code> to display just a summary of the GVRP statistics.	
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- "End of PDU" was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.
- The attribute that was being parsed had an invalid VLAN ID. The valid range is from 1 to 4095.

A failed registration can occur for the following reasons:

- Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
- An entry for a new GVRP VLAN could not be created in the GVRP database.

Example

```
Dell#show gvrp statistics int te 1/0

Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
Dell#
```

Related Commands

[show gvrp](#) — displays the GVRP configuration.

Internet Group Management Protocol (IGMP)

IGMP and IGMP snooping commands are supported by the Dell Networking OS on the switch.

This chapter contains the following sections:

- [IGMP Commands](#)
- [IGMP Snooping Commands](#)

IGMP Commands

Dell Networking OS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- Dell Networking OS supports protocol-independent multicast-sparse (PIM-SM) and protocol-independent source-specific multicast (PIM-SSM) include and exclude modes.
- IGMPv2 is the default version of IGMP on interfaces. You can configure IGMPv3 on interfaces. It is backward compatible with IGMPv2.
- On the S-Series, the maximum number of interfaces supported 31. On the S-Series, the maximum number of interfaces supported 31. On the S6000, the maximum number of interfaces supported 31. The Z9000 supports up to 95 interfaces.
- There is no hard limit on the maximum number of groups supported.
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
- An administrative command (`ip igmp version`) is added to manually set the IGMP version.
- All commands previously used for IGMPv2 are compatible with IGMPv3.

clear ip igmp groups

Clear entries from the group cache table.

Z9500

Syntax	<code>clear ip igmp groups [<i>group-address</i> <i>interface</i>]</code>	
Parameters	<i>group-address</i>	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
	<i>interface</i> <i>interface</i>	Enter the following keywords and slot/port or number information:

- For a Port-Channel interface, enter the keyword `port-channel` then the slot/port information. The range is from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` then the slot/port information. The range is from 1 to 4094.
- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results.

debug ip igmp

Enable debugging of IGMP packets.

Z9500

Syntax

```
debug ip igmp [group address | interface]
```

- To disable IGMP debugging, use the `no debug ip igmp [group address | interface]` command.
- To disable all debugging, use the `undebg all` command.

Parameters

<i>group-address</i>	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
<i>interface</i> <i>interface</i>	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

ip igmp access-group

To specify access control for packets, use this feature.

Z9500

Syntax `ip igmp access-group access-list`
To remove the feature, use the `no ip igmp access-group access-list` command.

Parameters ***access-list*** Enter the name of the extended ACL (16 characters maximum).

Defaults Not configured

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information The access list accepted is an extended ACL. To block IGMP reports from hosts, on a per-interface basis based on the group address and source address that you specify in the access list, use this feature.

ip igmp group-join-limit

To limit the number of IGMP groups that can be joined in a second, use this feature.

Z9500

Syntax	<code>ip igmp group-join-limit <i>number</i></code>	
Parameters	<i>number</i>	Enter the number of IGMP groups permitted to join in a second. The range is from 1 to 10000.
Defaults	none	
Command Modes	CONFIGURATION (conf-if- <i>interface-slot/port</i>)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on the E-Series.

ip igmp immediate-leave

Enable IGMP immediate leave.

Z9500

Syntax	<code>ip igmp immediate-leave [group-list <i>prefix-list-name</i>]</code> To disable <code>ip igmp immediate leave</code> , use the <code>no ip igmp immediate-leave</code> command.															
Parameters	group-list <i>prefix-list-name</i>	Enter the keywords <code>group-list</code> then a string up to 16 characters long of the <code>prefix-list-name</code> .														
Defaults	Not configured.															
Command Modes	INTERFACE															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
Version	Description															
9.5(0.1)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.8.1.0	Introduced on the S-Series.															
7.7.1.0	Introduced on the C-Series.															
Usage Information	Querier normally sends some group-specific queries when a <code>leave</code> message is received for a group prior to deleting a group from the membership database. There may be situations when you require immediate deletion of a group from the membership database. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable <code>immediate-leave processing</code> for specified groups.															

ip igmp last-member-query-interval

Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Z9500

Syntax	<code>ip igmp last-member-query-interval <i>milliseconds</i></code> To return to the default value, use the <code>no ip igmp last-member-query-interval</code> command.	
Parameters	<i>milliseconds</i>	Enter the number of milliseconds as the interval. The range is from 100 to 65535. The default is 1000 milliseconds .
Defaults	1000 milliseconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax	<code>ip igmp querier-timeout <i>seconds</i></code> To return to the default value, use the <code>no ip igmp querier-timeout</code> command.	
Parameters	<i>seconds</i>	Enter the number of seconds the router must wait to become the new querier. The range is from 60 to 300. The default is 125 seconds .

Defaults **125 seconds**

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

ip igmp query-interval

Change the transmission frequency of IGMP general queries the Querier sends.

Z9500

Syntax
`ip igmp query-interval seconds`
To return to the default values, use the `no ip igmp query-interval` command.

Parameters
seconds Enter the number of seconds between queries sent out. The range is from 1 to 18000. The default is **60 seconds**.

Defaults **60 seconds**

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

Z9500

Syntax	<code>ip igmp query-max-resp-time seconds</code> To return to the default values, use the <code>no ip igmp query-max-resp-time</code> command.	
Parameters	seconds	Enter the number of seconds for the maximum response time. The range is from 1 to 25. The default is 10 seconds .
Defaults	10 seconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.

Version	Description
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

ip igmp ssm-map

To translate (*,G) memberships to (S,G) memberships, use a statically configured list.

Z9500

Syntax

```
ip igmp ssm-map std-access-list source-address
```

Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) state, use the `ip igmp ssm-map std-access-list source-address` command.

Parameters

<i>std-access-list</i>	Specify the standard IP access list that contains the mapping rules for multicast groups.
<i>source-address</i>	Specify the multicast source address to which the groups are mapped.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the C-Series and S-Series.	7.7.1.0	Introduced on the E-Series.
Version	Description										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										
7.8.1.0	Introduced on the C-Series and S-Series.										
7.7.1.0	Introduced on the E-Series.										
Usage Information	Mapping applies to both v1 and v2 IGMP joins; any updates to the ACL are reflected in the IGMP groups. You may not use extended access lists with this command. When you configure a static SSM map and the router cannot find any matching access lists, the router continues to accept (*,G) groups.										
Related Commands	ip access-list standard — creates a standard access list to filter based on IP address.										

ip igmp static-group

Configure an IGMP static group.

Z9500

Syntax	<pre>ip igmp static-group {group address [exclude [source address]] [include {source address}]}</pre> To delete a static address, use the <code>no ip igmp static-group {group address [exclude [source address]] [include {source address}]}</code> command.	
Parameters	group address exclude source address include source address	Enter the group address in dotted decimal format (A.B.C.D). (OPTIONAL) Enter the keyword <code>exclude</code> then the source address, in dotted decimal format (A.B.C.D), for which a static entry is added. (OPTIONAL) Enter the keyword <code>include</code> then the source address, in dotted decimal format (A.B.C.D), for which a static entry is added.
Defaults	none	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.	

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Expanded to support the <code>exclude</code> and <code>include</code> options.

Usage Information

A group in `include` mode must have at least one source address defined. In `exclude` mode, if you do not specify a source address, The system implicitly assumes all sources are included. If you do not specify either `include` or `exclude`, the system implicitly assumes a IGMPv2 static join.

Command Limitations

- Only one mode (`include` or `exclude`) is permitted per multicast group per interface. To configure another mode, all sources belonging to the original mode must be unconfigured.
- If a static configuration is present and a packet for the same group arrives on an interface, the dynamic entry completely overwrites all the static configuration for the group.

Related Commands

[show ip igmp groups](#) — displays IGMP group information.

ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

Z9500

Syntax	<code>ip igmp version {2 3}</code>	
Parameters	2	Enter the number 2 to set the IGMP version number to IGMPv2.
	3	Enter the number 3 to set the IGMP version number to IGMPv3.
Defaults	2 (that is, IGMPv2)	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

show ip igmp groups

View the IGMP groups.

Z9500

Syntax

```
show ip igmp groups [group-address [detail] | detail |
interface [group-address [detail]]]
```

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
interface	(OPTIONAL) Enter the interface type and slot/port information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface enter the keyword <code>vlan</code> then a number from 1 to 4094.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to display the IGMPv3 source information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series and C-Series.
7.5.1.0	Expanded to support the <code>detail</code> option.

Usage Information

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the following example.

Field	Description
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Mode	Displays the IGMP version used.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.
Member Ports	Indicates the port channel. If the port channel is VLT, an asterisk (*) after the port channel number indicates the port channel is locally down and that a remote VLT port is up.

Example

```
Dell#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
225.0.0.0      Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.1      Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.2      Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.3      Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
```

```
225.0.0.4    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2
```

Example (VLT)



NOTE: The asterisk (*) after the port channel number (Po 2) highlighted in the following example indicates the port channel is VLT, that the local VLT port channel is down and the remote VLT port is up.

```
Dell#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
225.0.0.0    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.1    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.2    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.3    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.4    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
```

show ip igmp interface

View information on the interfaces participating in IGMP.

Z9500

Syntax

```
show ip igmp interface [interface]
```

Parameters

interface

(OPTIONAL) Enter the interface type and slot/port information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking TOS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results.

Example

```
Dell#show ip igmp interface
GigabitEthernet 0/0 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/5 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/6 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/7 is up, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 7/9 is up, line protocol is up
  Internet address is 10.87.5.250/24
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  IGMP last member query response interval is 1000 ms
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.87.5.250 (this system)
  IGMP version is 2
```

show ip igmp ssm-map

Display is a list of groups that are currently in the IGMP group table and contain SSM mapped sources.

Z9500

Syntax `show ip igmp ssm-map [group]`

Parameters

group	(OPTIONAL) Enter the multicast group address in the form A.B.C.D to display the list of sources to which this group is mapped.
--------------	--

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.7.1.0	Introduced on the E-Series.

**Related
Commands**

[ip igmp ssm-map](#) — uses a statically configured list to translate (*,G) memberships to (S,G) memberships.

IGMP Snooping Commands

IGMP Snooping version 2 and 3 are supported on the switch.

Important Points to Remember for IGMP Snooping

- The Dell Networking OS supports version 1, version 2, and version 3 hosts.
- The IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- The IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- The system supports IGMP snooping on JUMBO-enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.
- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes multiple spanning tree protocol (MSTP) triggers by sending a general query on the interface that comes in the FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is reassigned to the VLAN interface.
- When enabled, IGMP snooping Querier does not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it checks the IP source address of the incoming frame.

If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, the switch disables its IGMP snooping Querier functionality.

If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch continues to work as an IGMP snooping Querier.

ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This command is the master on/off switch to enable IGMP snooping.

Syntax `ip igmp snooping enable`
To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults Disabled.

Command Modes

- CONFIGURATION
- INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information To enable IGMP snooping, enter this command. When you enable this command from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN).



NOTE: Execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.

ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

Z9500

Syntax `ip igmp snooping fast-leave`
To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-n)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information Queriers normally send some queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a fast deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets.

Z9500

Syntax `ip igmp snooping flood`

Defaults Enabled.

Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series and S-Series.	7.7.1.0	Introduced on the E-Series.
Version	Description																
9.5(0.1)	Introduced on the Z9500.																
9.0.2.0	Introduced on the S6000.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.2.1.0	Introduced on the C-Series and S-Series.																
7.7.1.0	Introduced on the E-Series.																
Usage Information	On the C-Series and S-Series, unregistered multicast data traffic drops when you disable flooding; they do not forward the packets to multicast router ports. On the C-Series and S-Series, in order to disable Layer 2 multicast flooding, disable Layer 3 multicast (no ip multicast-routing).																

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

Z9500

Syntax	<pre>ip igmp snooping last-member-query-interval <i>milliseconds</i></pre> To return to the default value, use the <code>no ip igmp snooping last-member-query-interval</code> command.
Parameters	<i>milliseconds</i> Enter the interval in milliseconds. The range is from 100 to 65535. The default is 1000 milliseconds.
Defaults	1000 milliseconds
Command Modes	INTERFACE VLAN
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information This last-member-query-interval is also the interval between successive Group-Specific Query messages. To change the last-member-query interval, use this command.

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

Z9500

Syntax `ip igmp snooping mrouter interface interface`
 To delete a specific multicast router interface, use the `no igmp snooping mrouter interface interface` command.

Parameters

interface <i>interface</i>	Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. For the C-Series and S-Series, the range is from 1 to 128.
--------------------------------------	---

Defaults Not configured.

Command Modes INTERFACE VLAN — (conf-if-vl-*n*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

Dell Networking OS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

Z9500

Syntax

`ip igmp snooping querier`

To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.

Defaults

Not configured.

Command Modes

INTERFACE VLAN — (conf-if-vl-n)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information This command enables the IGMP switch to send General Queries periodically. This behavior is useful when there is no multicast router present in the VLAN because the multicast traffic is not routed. Assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

Display multicast router interfaces.

Z9500

Syntax `show ip igmp snooping mrouter [vlan number]`

Parameters

vlan number	Enter the keyword <code>vlan</code> then the vlan number. The range is from 1 to 4094.
--------------------	--

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information If the port channel is a VLT port channel, an asterisk (*) after the port channel number (Po 100*) indicates the port channel is locally down and that a remote VLT port is up.

Example

```
Dell#show ip igmp snooping mrouter
Interface Router Ports
```

```
Vlan 2 Te 1/3, Po 1  
Dell#
```

Related Commands

- [ip igmp snooping mrouter](#) — configures a static connection to the multicast router.
- [show ip igmp groups](#) — view groups.

Interfaces

The Dell Networking OS supports the interface configuration commands described in this chapter. This chapter contains the following sections:

- [Basic Interface Commands](#)
- [EIS Commands](#)
- [Port Channel Commands](#)
- [UDP Broadcast](#)

Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

clear counters

Clear the counters used in the show interfaces commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

Z9500

Syntax	<code>clear counters [<i>interface</i>] [vrrp [ipv6 {<i>vrid</i>} learning-limit]</code>	
Parameters	<i>interface</i>	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: • For IPv4 access-group counters, enter the keyword <code>ip</code>. • For IPv6 access-group counters, enter the keyword <code>ipv6</code>. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For MAC access-group counters, enter the keyword <code>mac</code>. • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For the management interface on the RPM, enter the keyword <code>ManagementEthernet</code> then slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a tunnel interface, enter the keyword <code>tunnel</code>. The range is from 1 to 16383.

	vrrp [[ipv6] vrid] (OPTIONAL) Enter the keyword <code>vrrp</code> to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter <code>ipv6</code>. To clear the counters of a specified group, enter a VRID number from 1 to 255. learning-limit (OPTIONAL) Enter the keywords <code>learning-limit</code> to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.																								
Defaults	Without an interface specified, the command clears all interface counters.																								
Command Modes	EXEC Privilege																								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.4.1.0</td><td>Added support (E-Series only) for VRRP groups in a VRF instance.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Added support for 4093 VLANs on the E-Series ExaScale. Prior to the release, 2094 was supported.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.5.1.0</td><td>Updated the definition of the <code>learning-limit</code> option for clarity.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.4.1.0	Added support (E-Series only) for VRRP groups in a VRF instance.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Added support for 4093 VLANs on the E-Series ExaScale. Prior to the release, 2094 was supported.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Updated the definition of the <code>learning-limit</code> option for clarity.
Version	Description																								
9.2(1.0)	Introduced on the Z9500.																								
8.3.19.0	Introduced on the S4820T.																								
8.3.11.1	Introduced on the Z9000.																								
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																								
8.4.1.0	Added support (E-Series only) for VRRP groups in a VRF instance.																								
8.3.7.0	Introduced on the S4810.																								
8.2.1.0	Added support for 4093 VLANs on the E-Series ExaScale. Prior to the release, 2094 was supported.																								
8.1.1.0	Introduced on the E-Series ExaScale.																								
7.6.1.0	Introduced on the S-Series.																								
7.5.1.0	Introduced on the C-Series.																								
6.5.1.0	Updated the definition of the <code>learning-limit</code> option for clarity.																								
Usage Information	After you enter the <code>clear counters</code> command, interface counters may not be increased in <code>show</code> command output for up to 20 seconds.																								
Example	<pre>Dell#clear counters Clear counters on all interfaces [confirm]</pre>																								
Related Commands	mac learning-limit — allows aging of MACs even though a learning-limit is configured or disallow station move on learned MACs. show interfaces — displays information on the interfaces.																								

clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

Z9500

Syntax	<code>clear dampening [interface]</code>	
Parameters	<i>interface</i>	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

Defaults	Without an interface specified, the command clears all interface dampening counters.
----------	--

Command Modes	EXEC Privilege
---------------	----------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example	<pre>Dell#clear dampening tengigabitethernet 1/2 Clear dampening counters on Te 1/2 [confirm] y Dell#</pre>
---------	---

Related
Commands

[show interfaces dampening](#) — displays interface dampening information.

[dampening](#) — configures dampening on an interface.

dampening

Configure dampening on an interface.

Z9500

Syntax

```
dampening [[[half-life] [reuse-threshold]] [suppress-  
threshold]] [max-suppress-time]
```

Parameters

<i>half-life</i>	Enter the number of seconds after which the penalty is decreased. The penalty decreases half after the half-life period expires. The range is from 1 to 30 seconds. The default is 5 seconds .
<i>reuse-threshold</i>	Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”. The range is from 1 to 20000. The default is 750 .
<i>suppress-threshold</i>	Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”. The range is from 1 to 20000. The default is 2500 .
<i>max-suppress-time</i>	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. The range is from 1 to 86400. The default is 20 seconds .

Defaults

Disabled.

Command
Modes

INTERFACE (conf-if-)

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.4.1.0	Introduced on the E-Series.
Version	Description				
7.4.1.0	Introduced on the E-Series.				
Usage Information	With each flap, the system penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface moves to the Error-Disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. After the penalty decays below the reuse threshold, the interface enables. The configured parameters are as follows: • <code>suppress-threshold</code> should be greater than <code>reuse-threshold</code> • <code>max-suppress-time</code> should be at least 4 times <code>half-life</code>  NOTE: You cannot apply dampening on an interface that is monitoring traffic for other interfaces.				
Example	<pre>Dell(config-if-te-2/2)#dampening 20 800 4500 120 Dell(config-if-te-2/2)#</pre>				
Related Commands	clear dampening — clears the dampening counters on all the interfaces or just the specified interface. show interfaces dampening — displays interface dampening information.				

description

Assign a descriptive text string to the interface.

Z9500

Syntax	<pre>description desc_text</pre> To delete a description, use the <code>no description</code> command.		
Parameters	<table> <tr> <td>desc_text</td><td>Enter a text string up to 240 characters long.</td></tr> </table>	desc_text	Enter a text string up to 240 characters long.
desc_text	Enter a text string up to 240 characters long.		
Defaults	none		
Command Modes	INTERFACE		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.		

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Modified for E-Series: Revised from 78 to 240 characters.

Usage Information

Important Points to Remember:

- To use special characters as a part of the description string, you must enclose the whole string in double quotes.
- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks ("*desc_text*").
- Entering a text string after the `description` command overwrites any previous text string that you previously configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

Related Commands

[show interfaces](#) — displays information about an interface.

duplex (Management)

Set the mode of the Management interface.

Z9500

Syntax

```
duplex {half | full}
```

To return to the default setting, use the `no duplex` command.

Parameters

half	Enter the keyword <code>half</code> to set the Management interface to transmit only in one direction.
full	Enter the keyword <code>full</code> to set the Management interface to transmit in both directions.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Documentation modified—added <i>Management</i> to distinguish from <i>duplex</i> (10/100 Interfaces).

Usage Information

This command applies only to the Management interface on the route processor modules (RPMs).

Related Commands

[interface ManagementEthernet](#) — configures the Management port on the system (either the Primary or Standby RPM).

[duplex \(Management\)](#) — sets the mode of the Management interface.

[management route](#) — configures a static route that points to the Management interface or a forwarding router.

[speed \(Management interface\)](#) — sets the speed on the Management interface.

flowcontrol

Enable and disable link-level flow control (802.3x pause frames) on an interface and (optionally) configure buffer thresholds for pause and offset frame transmission.

Z9500

Syntax

```
flowcontrol rx {off | on} tx {off | on} [pause-threshold {1-12480}] [resume-offset {1-12480}]
```

Parameters

rx on	Enter the keywords <code>rx on</code> to process the received flow control frames on this port.
rx off	Enter the keywords <code>rx off</code> to ignore the received flow control frames on this port.
tx on	Enter the keywords <code>tx on</code> to send control frames from the port to the connected device when a higher rate of traffic is received.
tx off	Enter the keywords <code>tx off</code> so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

	pause-threshold Enter the keyword <code>pause-threshold</code> to configure the buffer threshold (in Kilobytes) at which the interface starts transmitting pause frames for link-level flow control. Valid values are 1 to 12480KB. The default is 60KB. resume-offset Enter the keyword <code>resume-offset</code> to configure the buffer threshold (in Kilobytes) at which the interface resumes transmitting offset frames for link-level flow control. Valid values are 1 to 12480KB. The default is 9KB.																
Defaults	An interface ignores flow-control frames received from other network devices (rx off) and does not transmit pause frames (tx off).																
Command Modes	INTERFACE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>6.5.1.9/7.4.1.0</td><td>Introduced on the E-Series.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series with the <code>thresholds</code> option.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	6.5.1.9/7.4.1.0	Introduced on the E-Series.	7.8.1.0	Introduced on the C-Series and S-Series with the <code>thresholds</code> option.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.1.1.0	Introduced on the E-Series ExaScale.																
6.5.1.9/7.4.1.0	Introduced on the E-Series.																
7.8.1.0	Introduced on the C-Series and S-Series with the <code>thresholds</code> option.																
Usage Information	The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address. The pause: - Starts when <i>either</i> the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped. - Ends when <i>both</i> the packet pointer and the buffer threshold fall below 50% of the threshold settings. The <i>discard threshold</i> defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the switch. The discard threshold should be larger than the <i>buffer threshold</i> so that the buffer holds at least hold at least three packets. Changes in the flow-control values may not be reflected automatically in the <code>show interface</code> output. As a workaround, apply the new settings, execute <code>shut</code> then																

no shut on the interface, then check the running-config of the port using the show interface command.

Important Points to Remember

- Do not enable tx pause when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Asymmetric flow control (rx on tx off, or rx off tx on) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

```
Can't configure Asymmetric flowcontrol when speed <1G,  
config ignored
```

- The only configuration applicable to half duplex ports is rx off tx off. The following error is returned:

```
Can't configure flowcontrol when half duplex is configure,  
config ignored
```

- Half duplex cannot be configured when the flow control configuration is on (default is rx on tx on). The following error is returned:

```
Can't configure half duplex when flowcontrol is on, config  
ignored
```



NOTE: The flow control must be off (rx off tx off) before configuring the half duplex.



NOTE: If you use the disable rx flow control command, Dell Networking recommends rebooting the system.

Example

```
Dell(conf-if-te-0/1)#show config  
!  
interface TengigabitEthernet 0/1  
no ip address  
switchport  
no negotiation auto  
flowcontrol rx off tx on  
no shutdown  
...
```

Related Commands

[show running-config](#) — displays the flow configuration parameters (non-default values only).

[show interfaces](#) — displays the negotiated flow control parameters.

interface

Configure a physical interface on the switch.

Z9500

Syntax

```
interface interface range
```

Parameters

interface

Enter one of the following keywords and slot/port or number information:

- For a null interface, enter the keyword `null` then the slot/port information. The Null interface number is 0.
- For a Management Ethernet interface, enter the keyword `managementethernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then the slot/port information. The range is from 0 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then the slot/port information. The range is from 1 to 4094.

range (Optional) Enter the keyword `range` to configure an interface range.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Usage Information You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are not assigned to an IP address or switchport. To place an interface in Layer 2 mode, ensure that the interface's configuration does not contain an IP address and enter the `switchport` command.

You can create up to 64 tunnel interfaces. The tunnel is added as a logical interface with no default configuration. To delete a tunnel interface, use the `no interface tunnel tunnel-id` command.

Example

```
Dell(conf)#int tengigabitethernet 0/0
Dell(conf-if-te-0/0)#exit
Dell(conf)#
```

Related Commands

[interface loopback](#) — configures a Loopback interface.

[interface null](#) — configures a Null interface.

[interface port-channel](#) — configures a port channel.

[interface vlan](#) — configures a VLAN.

[show interfaces](#) — displays the interface configuration.

interface loopback

Configure a Loopback interface.

Z9500

Syntax

```
interface loopback number
```

To remove a loopback interface, use the `no interface loopback number` command.

Parameters

number

Enter a number as the interface number. The range is from 0 to 16383.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Example

```
Dell(config)#interface loopback 1655
Dell(config-if-lo-1655)#
```

Related Commands

[interface](#) — configures a physical interface.

[interface null](#) — configures a Null interface.

[interface port-channel](#) — configures a port channel.

[interface vlan](#) — configures a VLAN.

interface ManagementEthernet

Configure the Management port on the system (either the Primary or Standby RPM).

Z9500

Syntax	<code>interface ManagementEthernet slot/port</code>	
Parameters	slot/port	Enter the keyword <code>ManagementEthernet</code> , then the slot number (0 or 1) and port number zero (0).
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the S55, S60, and S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>6.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	6.4.1.0	Introduced
Version	Description				
6.4.1.0	Introduced				
Usage Information	You cannot delete a Management port. The Management port is enabled by default (<code>no shutdown</code>). To assign an IP address to the Management port, use the <code>ip address</code> command. If your system has two RPMs installed, use the <code>show redundancy</code> command to display which RPM is the Primary RPM.				
Example	<pre>Dell(config)#interface managementethernet 0/0 Dell(config-if-ma-0/0)#</pre>				
Related Commands	management route — configures a static route that points to the Management interface or a forwarding router. duplex (Management) — clears the forwarding information base (FIB) entries on a specified line card. speed (Management interface) — clears the FIB entries on a specified line card.				

interface null

Configure a Null interface on the switch.

Z9500

Syntax	<code>interface null <i>number</i></code>										
Parameters	<i>number</i> Enter zero (0) as the Null interface number.										
Defaults	Not configured; number = 0										
Command Modes	CONFIGURATION										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										

	Version	Description
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.4.1.0	Introduced
Usage Information	You cannot delete the Null interface. The only configuration command possible in a Null interface is <code>ip unreachable</code> .	
Example	<pre>Dell(conf)#interface null 0 Dell(conf-if-nu-0)#</pre>	
Related Commands	interface — configures a physical interface. interface loopback — configures a Loopback interface. interface port-channel — configures a port channel. interface vlan — configures a VLAN. ip unreachable — enables generation of internet control message protocol (ICMP) unreachable messages.	

interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

Z9500

Syntax	<code>interface range interface, interface,...</code>	
Parameters	<i>interface, interface,...</i>	Enter the keywords <code>interface range</code> and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, <code>interface range tengigabitethernet 0/1 - 5</code> is valid; <code>interface range tengigabitethernet 0/1-5</code> is NOT valid. • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a Tunnel interface, enter the keyword `Tunnel` then a number from 1 to 16383.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

Important Points to Remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.

- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

Example (Bulk)

```
Dell(conf)#interface range te 10/0, fo 0/0, te 2/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (Multiple Ports)

```
Dell(conf)#interface range te 2/0 - 23, te 2/1 - 10
Dell(conf-if-range-te-2/0-23#
```

Example (Overlapping Ports)

```
Dell(conf)#interface range te 2/1 - 11, te 2/1 - 23
Dell(conf-if-range-te-2/1-23#
```

Usage Information

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.



NOTE: If a range has VLAN, physical, and port-channel interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

Example (Single Range)

This example shows a single range bulk configuration.

```
Dell(config)# interface range tengigabitethernet 1/1 - 23
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add different interface types to the range enabling all 10-Gigabit Ethernet interfaces in the range 2/1 to 2/23 and both 10-Gigabit Ethernet interfaces 1/1 and 1/2.

```
Dell(config-if)# interface range tengigabitethernet 2/1-23,
tengigabitethernet 1/1-2
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add VLAN and port-channel interfaces to the range.

```
Dell(config-if)# interface range tengigabitethernet 2/1-23,
tengigabitethernet 1/1-2,
Vlan 2-100, Port 1-25
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```


Related
Commands

[interface port-channel](#) — configures a port channel group.

[interface vlan](#) — configures a VLAN interface.

[show config \(from INTERFACE RANGE mode\)](#) — shows the bulk configuration interfaces.

[show range](#) — shows the bulk configuration ranges.

[interface range macro \(define\)](#) — defines a macro for an interface-range.

interface range macro (define)

Defines a macro for an interface range and then saves the macro in the running configuration.

Z9500

Syntax

```
define interface range macro name interface , interface , ...
```

Parameters

name

Enter up to 16 characters for the macro name.

interface,
interface,...

Enter the keywords `interface range` and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces.

Slot/Port information must contain a space before and after the dash. For example, `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is NOT valid.

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults

none

Command
Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Single Range)

This example shows how to define an interface range macro named test. Execute the `show running-config` command to display the macro definition.

```
Dell(config)# define interface-range test tengigabitethernet
0/0-3,
tengigabitethernet 1/0-47, tengigabitethernet 2/0-89
```

```
Dell# show running-config | grep define
define interface-range test tengigabitethernet 0/0-3,
tengigabitethernet 1/0-47,
tengigabitethernet 2/0-89
```

```
Dell(config)#interface range macro test
Dell(config-if-range-te-0/0-3,te-1/0-47,te-2/0-89) #
```

Related Commands

[interface range](#) – configures a range of command (bulk configuration)

[interface range macro name](#) – runs an interface range macro.

interface range macro name

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

Z9500

Syntax

```
interface range macro name
```

Parameters

name Enter the name of an existing macro.

Defaults	none																		
Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.2.1.0	Introduced																		
Example (Single Range)	This example displays the macro named <code>test</code>. <pre>Dell(config)#interface range macro test Dell(config-if-range-te-0/0-3,te-1/0-47,te-2/0-89)# Dell</pre>																		
Related Commands	interface range — configures a range of command (bulk configuration). interface range macro (define) — defines a macro for an interface range (bulk configuration).																		

interface vlan

Configure a VLAN. You can configure up to 4094 VLANs.

Z9500

Syntax	<code>interface vlan <i>vlan-id</i></code>
Parameters	<i>vlan-id</i> Enter a number as the VLAN Identifier. The range is 1 to 4094.
Defaults	Not configured, except for the Default VLAN, which is configured as VLAN 1.
Command Modes	CONFIGURATION

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	9.0(1.3)	Introduced on the S5000.
Usage Information	For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands section of the Layer 2 chapter. FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC ACLs are not supported in VLANs. IP ACLs are supported. For more information, refer to the Access Control Lists (ACL) chapter.	
Example (Single Range)	<pre>Dell(conf)#int vlan 3 Dell(conf-if-vl-3)#</pre>	
Related Commands	interface – configures a physical interface. interface loopback – configures a loopback interface. interface null – configures a null interface. interface port-channel – configures a port channel group. show vlan – displays the current VLAN configuration on the switch. shutdown – disables/enables the VLAN. tagged – adds a Layer 2 interface to a VLAN as a tagged interface. untagged – adds a Layer 2 interface to a VLAN as an untagged interface.	

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Z9500

Syntax	<pre>keepalive [seconds]</pre> To stop sending keepalive packets, use the <code>no keepalive</code> command.	
Parameters	seconds	(OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is 10 seconds .
Defaults	Enabled.	
Command Modes	INTERFACE	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

linecard portmode

Split a single 40G port into four 10G ports on the switch.

Z9500

Syntax

```
linecard slot-id port number portmode quad
```

Parameters

linecard <i>slot-id</i>	Enter the slot ID of a Z9500 line card to reset. The range of slot IDs is from 0 to 2.
<i>number</i>	Enter the port number of the 40G port to be split. A 40G port number is a multiple of 4; for example, 0, 4, 8, 12, ... 120, 124, 128).

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				
Usage Information	Enabling quad mode on a port removes the interface configurations (if any) on the port after a save and reload. Be sure that the port is removed from other L2 and L3 feature configurations. You must save and reload the system for the 40G to 4x10G port change to take effect. This command cannot be used if LR4 optics are inserted in the 40G port.				

monitor interface

Monitor counters on a single interface or all interfaces on a line card. The screen is refreshed every five seconds and the CLI prompt disappears.

Z9500

Syntax	<pre>monitor interface [<i>interface</i>] [<i>linecard slot-id</i>]</pre> To disable monitoring and return to the CLI prompt, press the <code>q</code> key.	
Parameters	<i>interface</i> (OPTIONAL) Enter the following keywords and slot/port or number information: • For the management port, enter the keyword <code>managementethernet</code> then the slot (0 or 1) and the port (0). • For a Tunnel interface, enter the keyword <code>tunnel</code> then the slot/port. The range is from 1 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> then the slot/port. The range is from 1 to 4094.	
	<i>linecard slot-id</i> Enter the <code>linecard slot-id</code> parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.	
Command Modes	• EXEC • EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

In the Examples, the delta column displays changes since the last screen refresh. The following are the `monitor` command menu options.

Key	Description
systest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the <code>monitor interface</code> command was entered.
time	Displays the amount of time the chassis is up (since last reboot).
m	Change the view from a single interface to all interfaces on the line card or visa-versa.
c	Refresh the view.
b	Change the counters displayed from Packets on the interface to Bytes.
r	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
l	Change the view to the next interface on the line card, or if in line card mode, the next line card in the chassis.
a	Change the view to the previous interface on the line card, or if in line card mode, the previous line card in the chassis.
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

Example

```
Dell# monitor interface fortyGigE 2

Dell Networking operating system uptime is 3 minute(s)
Monitor time: 00:00:00   Refresh Intvl.: 2s

Interface   Link           In Packets      [delta]
```

Out	Packets		[delta]	
0	Fo 2/4	Up	2	0
0	Fo 2/8	Down	0	0
0	Fo 2/12	Down	0	0
0	Fo 2/16	Up	1	0
0	Fo 2/20	Up	1	0
0	Fo 2/24	Down	0	0
0	Fo 2/28	Up	1	0
0	Fo 2/32	Up	2	0
0	Fo 2/36	Down	0	0
0	Fo 2/40	Up	2	0
0	Fo 2/44	Up	2	0
0	Fo 2/48	Down	0	0
0	Fo 2/52	Down	0	0
0	Fo 2/56	Down	0	0
0	Fo 2/60	Down	0	0
0	Fo 2/64	Down	0	0
0	Fo 2/68	Down	0	0
0	Fo 2/72	Down	0	0
0	Fo 2/76	Down	0	0
0	Fo 2/80	Down	0	0
0	Fo 2/84	Down	0	0
0	Fo 2/88	Down	0	0
0	Fo 2/92	Down	0	0
0	Fo 2/96	Down	0	0

m - Change mode	c - Clear
screen	
b - Display bytes	r - Display
pkts/bytes per sec	
l - Page up	a - Page down
T - Increase refresh interval	t - Decrease
refresh interval	
q - Quit	

Dell# monitor interface

Dell Networking operating system uptime is 9 minute(s)
Monitor time: 00:00:00 Refresh Intvl.: 2s

Interface	Link	In Packets	[delta]
0 Te 1/0	Down	0	0
0 Te 1/1	Down	0	0
0 Te 2/2	Down	0	0
0 Te 2/3	Down	0	0
0 Fo 2/4	Up	12	0
0 Fo 2/8	Down	0	0
0 Fo 1/12	Down	0	0
0 Fo 1/16	Up	11	0
0 Fo 1/20	Up	11	0
0 Fo 2/24	Down	0	0
0 Fo 2/28	Up	12	0
0 Fo 2/32	Up	11	0
0 Fo 2/36	Down	0	0
0 Fo 2/40	Up	0	0
0 Fo 2/44	Up	13	0
0 Ma 0/0	Down	17	0

m - Change mode
 screen
 b - Display bytes
 pkts/bytes per sec
 l - Page up
 T - Increase refresh interval
 refresh interval
 q - Quit

c - Clear
 r - Display
 a - Page down
 t - Decrease

Dell# monitor interface managementethernet 0/0

Dell Networking operating system uptime is 4 minute(s)
 Monitor time: 00:00:00 Refresh Intvl.: 2s

Interface: Ma 0/0, Enabled, Link is Down, Linespeed is auto

Traffic statistics:	Current
Rate Delta	
Input bytes:	0 0
Bps Output bytes:	42 0
Bps Input packets:	6 0
pps Output packets:	1 0
pps 64B packets:	0 0
pps Over 64B packets:	0 0

```

pps          0
  Over 127B packets:      0      0
pps          0
  Over 255B packets:     0      0
pps          0
  Over 511B packets:     0      0
pps          0
  Over 1023B packets:    0      0
pps          0
  Error statistics:
00:04:36: %RPM0-P:CP %CHMGR-5-PEM_INSERTED: Power entry module
3 of unit 0 is inserted
  Input underruns:      0      0
pps          0
  Input giants:        0      0
pps          0
00:04:36: %RPM0-P:CP %CHMGR-0-PS_UP: Power supply 3 in unit 0
is up
  Input throttles:     0      0
pps          0
  Input CRC:           0      0
pps          0
  Input IP checksum:   0      0
pps          0
  Input overrun:      0      0
pps          0
  Output underruns:   0      0
pps          0
  Output throttles:   0      0
pps          0

      m - Change mode                      c - Clear
screen
      l - Page up                          a - Page down
      T - Increase refresh interval        t - Decrease
refresh interval
      q - Quit

```

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

Z9500

Syntax

`mtu value`

To return to the default MTU value, use the `no mtu` command.

Parameters

value

Enter a maximum frame size in bytes. The range is from 592 to 9216. The default is **9216**.

Defaults

9216

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header.

When you enter the `no mtu` command, the system reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following shows the difference between Link MTU and IP MTU.

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes

Layer 2 Overhead	Link MTU and IP MTU Delta
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

portmode hybrid

To accept both tagged and untagged frames, set a physical port or port-channel. A port configured this way is identified as a hybrid port in report displays.

Z9500

Syntax `portmode hybrid`
To return a port to accept either tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

Defaults non-hybrid

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The following describes the `interface` command shown in the following example. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port now accepts:

- untagged frames and classify them as VLAN 10 frames

- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the following example. This example shows output with "Hybrid" as the newly added value for 802.1QTagged. The options for this field are:

- True — port is tagged
- False — port is untagged
- Hybrid — port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the following example. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.



NOTE: Remove all other configurations on the port before you can remove the hybrid configuration from the port.

Example

```
Dell(conf)#interface te 2/0
Dell(conf-if-te-2/0)#portmode hybrid
Dell(conf-if-te-2/0)#interface vlan 10
Dell(conf-if-vl-10)#untagged te 2/0
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#tagged te 2/0
Dell(conf-if-vl-20)#
```

Example

```
Dell(conf-if-vl-20)#do show interfaces switchport
Name: TenGigabitEthernet 2/0
802.1QTagged: Hybrid
Vlan membership:
Vlan 10, Vlan 20
Native VlanId: 10
Dell(conf-if-vl-20)#
```

Example (Vlan)

```
Dell(conf-if-vl-20)#interface vlan 10
Dell(conf-if-vl-10)#no untagged te 2/0
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#no tagged te 2/0
Dell(conf-if-vl-20)#interface te 2/0
Dell(conf-if-te-2/0)#no portmode hybrid
Dell(conf-if-vl-20)#
```

Related Commands

[show interfaces switchport](#) — displays the configuration of switchport (Layer 2) interfaces on the switch.

[switchport](#) — places the interface in a Layer 2 mode.

[vlan-stack trunk](#) — specifies an interface as a trunk port to the Stackable VLAN network.

reset linecard

Reset the ports on a Z9500 line card.

Z9500

Syntax	<code>reset linecard slot-id</code>	
Parameters	linecard slot-id	Enter the slot ID number to specify the set of line-card ports to be reset. The range of Z9500 line-card slot IDs is 0 to 2.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell NetworkingOS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Added the <code>hard reset</code> option.
7.8.1.0	Augmented to run on the standby unit in order to reset the standby unit directly.
7.7.1.0	Introduced on the S-Series.

Usage Information	Resetting is a soft reboot, including flushing the forwarding tables.
--------------------------	---

Example	<pre>Stack MAC : 00:01:e8:8b:1a:36 Reload-Type : normal-reload [Next boot : normal-reload] -- Stack Info -- Unit UnitType Status ReqTyp CurTyp Version Ports ----- 0 Management online S4810 S4810 8-3-12-1 64 1 Standby online S4810 S4810 8-3-12-1 64 2 Member online S4810 S4810 8-3-12-1 64 3 Member online S4810 S4810 8-3-12-1 64 4 Member online S4810 S4810 8-3-12-1 64 5 Member online S4810 S4810 8-3-12-1 64 6 Member not present 7 Member not present 8 Member not present 9 Member not present 10 Member not present 11 Member not present</pre>
----------------	---

Related
Commands

- [reload](#) – reboots the Dell Networking OS.

show config

Display the interface configuration.

Z9500

Syntax `show config`

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if)#show conf
!
interface TenGigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
Dell(conf-if)#
```

show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (`interface range`).

Z9500

Syntax `show config`

Command Modes CONFIGURATION INTERFACE (conf-if-range)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf)#interface range tengigabitethernet 1/1 - 2
Dell(conf-if-range-te-1/1-2)#show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  no shutdown
!
interface TenGigabitEthernet 1/2
  no ip address
  switchport
  no shutdown
Dell(conf-if-range-te-1/1-2)#
```

show interfaces

Display information on a specific physical interface or virtual interface, or the interfaces of the same type on a line card.

Z9500

Syntax

```
show interfaces [interface] [linecard slot-id]
```

Parameters

interface

Enter one of the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.

linecard *slot-id* Enter the `linecard slot-id` parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for the tunnel interface type.
9.1(0.0)	Updated ManagementEthernet output to include two global IPv6 addresses on S4810 and Z9000 and added output example showing OpenFlow instance ID.
8.3.12.1	Updated command output to support multiple IPv6 addresses on S4810.
8.3.11.4	Output expanded to support eSR4 optics in Z9000.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.2	Included SFP and SFP+ optics power detail in the E-Series and C-Series output.
8.2.1.0	Added support for 4093 VLANs on the E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Output expanded to include SFP+ media on the C-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Changed the organization of the display output.

Version	Description
6.3.1.0	Added the Pluggable Media Type field in the E-Series TeraScale output.

Usage Information

Use the `show interfaces` command for details on a specific interface. Use the `show interfaces linecard` command for details on all interfaces on the designated line card.



NOTE: In the CLI output, the power value is rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an `snmp query` returns the corresponding dbm value even though the CLI displays as 0.000.



NOTE: After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there is no change in the line-rate.

User Information

The following table describes the `show interfaces` command shown in the 10G example below.

Line	Description
TenGigabitEthernet 0/0...	Interface type, slot/port, and administrative and line protocol status.
Hardware is...	Interface hardware information, assigned MAC address, and current address.
Pluggable media present...	Present pluggable media wavelength, type, and rate. The error scenarios are: - Wavelength, Non-qualified — Dell Force10 ID is not present, but wavelength information is available from XFP or SFP serial data - Wavelength, F10 unknown—Dell Force10 ID is present, but not able to determine the optics type - Unknown, Non-qualified— if wavelength is reading error, and F10 ID is not present Dell Networking allows unsupported SFP and XFP transceivers to be used, but the system might not be able to retrieve some data about them. In that case, typically when the output of this field is "Pluggable media present, Media type is unknown", the Medium and the XFP/SFP receive power reading data might not be present in the output.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU information.

Line	Description
LineSpeed	Displays the interface's line speed, duplex mode, and Slave.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the <code>show interfaces</code> counters were cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • Number of packets and bytes into the interface • Number of packets with VLAN tagged headers • Packet size and the number of those packets inbound to the interface • Number of Multicast and Broadcast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets • Number of runs, giants, and throttles packets: – runs = number of packets that are less than 64B – giants = packets that are greater than the MTU size – throttles = packets containing PAUSE frames • Number of CRC, overrun, and discarded packets: – CRC = packets with CRC/FCS errors – overrun = number of packets discarded due to FIFO overrun conditions – discarded = the sum of runs, giants, CRC, and overrun packets discarded without any processing
Output Statistics:	Displays output statistics sent out of the interface including: • Number of packets, bytes, and underruns out of the interface • Packet size and the number of those packets outbound to the interface • Number of Multicast, Broadcast, and Unicast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets – Unicasts = number of MAC unicast packets • Number of VLANs, throttles, discards, and collisions:: – Vlan = number of VLAN tagged packets – throttles = packets containing PAUSE frames – discarded = number of packets discarded without any processing

Line	Description
	- collisions = number of packet collisions - wred=count both packets discarded in the MAC and in the hardware-based queues
Rate information...	Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

Example

```

Dell# show interfaces
TenGigabitEthernet 2/0 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
Wavelength is 0.00nm
Interface index is 151060994
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:08:58
Queueing strategy: fifo
Input Statistics:
    0 packets, 0 bytes
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:
    0 packets, 0 bytes, 0 underruns
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
    Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
Time since last interface status change: 00:07:34

```

Usage Information

The Management port is enabled by default (no shutdown). If necessary, use the `ip address` command to assign an IP address to the Management port. If two RPMs are installed in your system, use the `show redundancy` command to display which RPM is the Primary RPM.

You can configure two global IPv6 addresses. To view the addresses, use the `show interface managementethernet` command. If you try to configure a third IPv6

address, a message displays. If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. The first IPv6 address that is configured on the management interface will be the primary address. If deleted, it must be re-added; the secondary address is not promoted.

**Example
(TenGigabit
Interface)**

```
Dell# show interfaces tengigabitethernet 2
TenGigabitEthernet 2/0 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
Wavelength is 0.00nm
Interface index is 151060994
Backup Interface of this port is Te 2/1
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:49
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
Time since last interface status change: 01:21:35
```

```
TenGigabitEthernet 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
Wavelength is 0.00nm
Interface index is 151323138
Backup Interface of this port is Te 2/0
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:49
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
```

```

byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
Time since last interface status change: 01:21:35

TenGigabitEthernet 2/2 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
  Current address is 74:86:7a:ff:6f:18
--More--

```

Example (VLAN Interface)

```

Dell# show interfaces vlan 1
Vlan 1 is down, line protocol is down
Address is 74:86:7a:ff:6f:18, Current address is 74:86:7a:ff:
6f:18
Interface index is 1124302849
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:55
Queueing strategy: fifo
Time since last interface status change: 01:22:55

```

Example (ManagementEthernet Interface with two IPv6 addresses)

```

Dell# show interfaces managementethernet 0/0

ManagementEthernet 0/0 is up, line protocol is up

Hardware is DellForce10Eth, address is 00:01:e8:a0:bf:f3

Current address is 00:01:e8:a0:bf:f3

Pluggable media not present

Interface index is 302006472

Internet address is 10.16.130.5/16

Link local IPv6 address: fe80::201:e8ff:fea0:bff3/64

Global IPv6 address: 1::1/

Global IPv6 address: 2::1/64

Virtual-IP is not set

```

```
Virtual-IP IPv6 address is not set

MTU 1554 bytes, IP MTU 1500 bytes

LineSpeed 1000 Mbit, Mode full duplex

ARP type: ARPA, ARP Timeout 04:00:00

Last clearing of "show interface" counters 00:06:14

Queueing strategy: fifo

Input 791 packets, 62913 bytes, 775 multicast

Received 0 errors, 0 discarded

Output 21 packets, 3300 bytes, 20 multicast

Output 0 errors, 0 invalid protocol

Time since last interface status change: 00:06:03
```

Related Commands

[show interfaces configured](#) – displays any interface with a non-default configuration.

[show interfaces phy](#)

[show interfaces switchport](#) – displays Layer 2 information about the interfaces.

[show inventory \(S-Series and Z-Series\)](#) – displays the S-Series and Z-Series switch types, components (including media), Dell Networking OS version including hardware identification numbers, and configured protocols.

[show ip interface](#) – displays Layer 3 information about the interfaces.

[show range](#) – displays all interfaces configured using the interface range command.

show interfaces configured

Display any interface with a non-default configuration.

Z9500

Syntax

```
show interfaces configured
```

Command Modes

- EXEC
- EXEC Privilege

**Command
History**

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Changed the organization of the display output.

Example

```
Dell# show interfaces configured
TenGigabitEthernet 2/0 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
  Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
  Wavelength is 0.00nm
Interface index is 151060994
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:47:42
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
Time since last interface status change: 01:46:17

TenGigabitEthernet 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
  Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
  Wavelength is 0.00nm
Interface index is 151323138
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
```

```

LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:47:42
Queueing strategy: fifo
Input Statistics:
    0 packets, 0 bytes
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:
    0 packets, 0 bytes, 0 underruns
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts, 0 Unicasts
    0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
    Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate
Time since last interface status change: 01:46:17

```

```

TenGigabitEthernet 2/2 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
    Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
    Wavelength is 0.00nm
--More--

```

Related Commands [show interfaces](#) — displays information on a specific physical interface or virtual interface.

show interfaces dampening

Display interface dampening information.

Z9500

Syntax `show interfaces dampening [[interface] [linecard slot-id]
[summary] [detail]]`

Parameters

interface (Optional) Enter one of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

linecard <i>slot-id</i>	Enter the <code>linecard slot-id</code> parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to display detailed interface dampening data.
Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Example

```
Dell# show interfaces dampening tengigabitethernet 2
Interface      Supp   Flaps   Penalty Half-Life   Reuse
Suppress      Max-Sup
State
Te 2/0         Up      0        0          5           200
250           300

Dell# show interfaces dampening summary
1 interface is configured with dampening. No interfaces are
currently suppressed.

Dell# show interfaces dampening detail

Interface                               : TenGigabitEthernet 2/0
Operation state                         : down
Suppression state                       : Up
Flap count                             : 0
Penalty                                : 0
Half life                               : 5
```

```

Reuse threshold                : 200
Suppression threshold         : 250
Max suppression time           : 300
Time since last suppressed     : 0
Time remaining to change state to up : 0

```

Related Commands

[dampening](#) — configures dampening on an interface.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

[show interfaces configured](#) — displays any interface with a non-default configuration.

show interfaces phy

Display auto-negotiation and link partner information.

Z9500

Syntax `show interfaces {tengigabitethernet | fortyGigE} slot/port phy`

Parameters

<code>{tengigabitethernet fortyGigE}</code>	Enter one of the keywords <code>tengigabitethernet</code> or <code>fortyGigE</code> with slot/port information.
---	---

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.
6.5.4.0	Introduced on the E-Series.

Usage Information The following describes the `show interfaces tengigabitethernet` command following example.

Mode Control	Indicates if <code>auto negotiation</code> is enabled. If so, indicates the selected speed and duplex.
Mode Status	Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the <code>autoNegComplete</code> field and the <code>linkstatus</code> field read "True."
AutoNegotiation Advertise	Displays the control words the local interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the local interface supports.
AutoNegotiation Remote Partner's Ability	Displays the control words the remote interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the remote interface supports.
AutoNegotiation Expansion	ParallelDetectionFault is the handshaking scheme in which the link partner continuously transmit an "idle" data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner or else no link can be established.
1000Base-T Control	1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting a speed to 1000 Mbps with the <code>speed</code> command without auto-negotiation. E-Series line cards support both full-duplex and half-duplex 1000BaseT.
Phy Specific Control	Values are: • 0 - Manual MDI • 1 - Manual MDIX • 2 - N/A • 3 - Auto MDI/MDIX
Phy Specific Status	Displays PHY-specific status information. Cable length represents a rough estimate in meters: • 0 - < 50 meters • 1 - 50 - 80 meters • 2 - 80 - 110 meters • 3 - 110 - 140 meters • 4 - 140 meters Link Status: Up or Down Speed: • Auto • 1000MB

- 100MB
- 10MB

Example

```
Dell#show int tengigabitethernet 1/0 phy
Mode Control:
  SpeedSelection:      10b
  AutoNeg:             ON
  Loopback:           False
  PowerDown:          False
  Isolate:             False
  DuplexMode:         Full
Mode Status:
  AutoNegComplete:    False
  RemoteFault:        False
  LinkStatus:         False
  JabberDetect:       False
AutoNegotiation Advertise:
  100MegFullDplx:     True
  100MegHalfDplx:     True
  10MegFullDplx:      False
  10MegHalfDplx:      True
  Asym Pause:         False
  Sym Pause:          False
AutoNegotiation Remote Partner's Ability:
  100MegFullDplx:     False
  100MegHalfDplx:     False
  10MegFullDplx:      False
  10MegHalfDplx:      False
  Asym Pause:         False
  Sym Pause:          False
AutoNegotiation Expansion:
  ParallelDetectionFault: False
...
```

Related Commands

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

show interfaces status

To display status information on a specific interface only, display a summary of interface information or specify a line card slot and interface.

Z9500

Syntax

```
show interfaces [interface | linecard slot-number] status
```

Parameters

interface

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then the slot/port information. The range is from 0 to 16383.

- For a Port-Channel interface, enter the keyword `port-channel` then the slot/port information. The range is from 0 to 128.

linecard slot-number (OPTIONAL) Enter the keyword `linecard` then the slot number.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Example

```
Dell#show interfaces status
Port      Description  Status  Speed    Duplex  Vlan
Te 2/0    Down        10000   Mbit    Auto    1
Te 2/1    Down        10000   Mbit    Auto    --
Te 2/2    Down        10000   Mbit    Auto    --
Te 2/3    Down        10000   Mbit    Auto    --
Fo 2/4    Down        40000   Mbit    Auto    --
Fo 2/8    Down        40000   Mbit    Auto    --
Fo 2/12   Down        40000   Mbit    Auto    --
Fo 2/16   Down        40000   Mbit    Auto    --
Fo 2/20   Down        40000   Mbit    Auto    --
Fo 2/24   Down        40000   Mbit    Auto    --
Fo 2/28   Down        40000   Mbit    Auto    --
Fo 2/32   Down        40000   Mbit    Auto    --
Fo 2/36   Down        40000   Mbit    Auto    --
Fo 2/40   Down        40000   Mbit    Auto    --
Fo 2/44   Down        40000   Mbit    Auto    --
Fo 2/48   Down        40000   Mbit    Auto    --
Fo 2/52   Down        40000   Mbit    Auto    --
Fo 2/56   Down        40000   Mbit    Auto    --
Fo 2/60   Down        40000   Mbit    Auto    --
Fo 2/64   Down        40000   Mbit    Auto    --
```

Fo 2/68	Down	40000	Mbit	Auto	--
Fo 2/72	Down	40000	Mbit	Auto	--
Fo 2/76	Down	40000	Mbit	Auto	--
Fo 2/80	Down	40000	Mbit	Auto	--
Fo 2/84	Down	40000	Mbit	Auto	--
Fo 2/88	Down	40000	Mbit	Auto	--
Fo 2/92	Down	40000	Mbit	Auto	--
Fo 2/96	Down	40000	Mbit	Auto	--
Fo 2/100	Down	40000	Mbit	Auto	--
Fo 2/104	Down	40000	Mbit	Auto	--
Fo 2/108	Down	40000	Mbit	Auto	--
Fo 2/112	Down	40000	Mbit	Auto	--
Fo 2/116	Down	40000	Mbit	Auto	--
Fo 2/120	Down	40000	Mbit	Auto	--
Fo 2/124	Down	40000	Mbit	Auto	--
Fo 2/128	Down	40000	Mbit	Auto	--
Fo 2/132	Down	40000	Mbit	Auto	--
Fo 2/136	Down	40000	Mbit	Auto	--
Fo 2/140	Down	40000	Mbit	Auto	--
Fo 2/144	Down	40000	Mbit	Auto	--
Fo 2/148	Down	40000	Mbit	Auto	--
Fo 2/152	Down	40000	Mbit	Auto	--
Fo 2/156	Down	40000	Mbit	Auto	--
Fo 2/160	Down	40000	Mbit	Auto	--
Fo 2/164	Down	40000	Mbit	Auto	--
Fo 2/168	Down	40000	Mbit	Auto	--
Fo 2/172	Down	40000	Mbit	Auto	--
Fo 2/176	Down	40000	Mbit	Auto	--
Fo 2/180	Down	40000	Mbit	Auto	--
Fo 2/184	Down	40000	Mbit	Auto	--
Fo 2/188	Down	40000	Mbit	Auto	--

Related Commands

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

Z9500

Syntax

```
show interfaces switchport [interface] [linecard slot-id]
```

Parameters

interface

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- Enter the keyword `backup` to view the backup interface for this interface.

linecard *slot-id* Enter the `linecard slot-id` parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Support added for hybrid port/native VLAN, introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show interfaces switchport` command for the following example.

Items	Description
Name	Displays the interface's type, slot, and port number.
802.1QTagged	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid"), which supports both untagged and tagged VLANs by port 13/0.
Vlan membership	Lists the VLANs to which the interface is a member.

Example

```
Dell#show interfaces switchport

Codes:  U - Untagged, T - Tagged
        x - Dot1x untagged, X - Dot1x tagged
        G - GVRP tagged, M - Trunk
        i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged

Name: TenGigabitEthernet 2/0
802.1QTagged: False
Vlan membership:
Q          Vlans
```

```

U          1

Name: Port-channel 23
802.1QTagged: False
Vlan membership:
Q          Vlans
U          1

Dell# show interfaces switchport tengigabitethernet 2

Codes:  U - Untagged, T - Tagged
        x - Dot1x untagged, X - Dot1x tagged
        G - GVRP tagged, M - Trunk
        i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged

Name: TenGigabitEthernet 2/0
802.1QTagged: False
Vlan membership:
Q          Vlans
U          1

Name: TenGigabitEthernet 2/1
802.1QTagged: False
Vlan membership:
Q          Vlans
U          1

```

Related Commands

[interface](#) — configures a physical interface on the switch.

[show ip interface](#) — displays Layer 3 information about the interfaces.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

[show interfaces transceiver](#) — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show interfaces transceiver

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

Z9500

Syntax	<code>show interfaces [tengigabitethernet <i>slot/port</i> fortyGigE <i>slot/port</i>] transceiver</code>	
Parameters	tengigabitether net	For a 10G interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information.
	fortyGigE	For a 40G interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Command Modes	EXEC	

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Output augmented with diagnostic data for pluggable media.
7.7.1.0	Removed three fields in the output: Vendor Name, Vendor OUI, and Vendor PN.
7.6.1.0	Introduced on the C-Series and S-Series.
6.5.4.0	Introduced on the E-Series.

Usage Information

The following describes the `show interfaces transceiver` command shown in the following example.

Line	Description
Rx Power measurement type	Output depends on the vendor, typically either "Average" or "OMA" (Receiver optical modulation amplitude).
Temp High Alarm threshold	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
Voltage High Alarm threshold	Displays the interface index number used by SNMP to identify the interface.
Bias High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.

Line	Description
Voltage Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temperature	Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.
Voltage	Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/warning flag is set to true.
Tx Bias Current	Present transmission (Tx) bias current of the SFP. If this crosses bias high alarm/warning thresholds, the TX bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the TX bias low alarm/warning flag is set to true.

Line	Description
Tx Power	Present Tx power of the SFP. If this crosses Tx power alarm/warning thresholds, the Tx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Tx power low alarm/warning flag is set to true.
Rx Power	Present receiving (Rx) power of the SFP. This value is either average Rx power or OMA. This depends on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Rx power low alarm/warning flag is set to true.
Data Ready state Bar	This field indicates that the transceiver has achieved power up and data is ready. This is set to true if data is ready to be sent and set to false if data is being transmitted.
Rx LOS state	This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.
Tx Fault state	This is the digital state of the Tx Fault output pin.
Rate Select state	This is the digital state of the SFP rate_select input pin.
RS state	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
Tx Disable state	If the admin status of the port is down then this flag is set to true.
Temperature High Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Voltage High Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Tx Bias High Alarm Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power High Alarm Flag	This can be either true or false, depending on the Current Tx bias power value displayed above.
Rx Power High Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias Low Alarm Flag	This can be either true or false, depending on the Tx bias current value displayed above.

Line	Description
Tx Power Low Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature High Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage High Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias High Warning Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias Low Warning Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power Low Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.

Example

```

Dell#show interfaces tengigabitethernet 1/0 transceiver
SFP is present.

SFP 0 Serial Base ID fields
SFP 0 Id = 0x03
SFP 0 Ext Id = 0x04
SFP 0 Connector = 0x07
SFP 0 Transceiver Code = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c
0x05
SFP 0 Encoding = 0x01
SFP 0 BR Nominal = 0x15
SFP 0 Length(9um) Km = 0x00
SFP 0 Length(9um) 100m = 0x00
SFP 0 Length(50um) 10m = 0x1e
SFP 0 Length(62.5um) 10m = 0x0f
SFP 0 Length(Copper) 10m = 0x00
SFP 0 Vendor Rev = A
SFP 0 Laser Wavelength = 850 nm
SFP 0 CheckCodeBase = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options = 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0

```

```

SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode      = 040528
SFP 0 CheckCodeExt  = 0x5b

SFP 1 Diagnostic Information
=====
SFP 1 Rx Power measurement type      = Average
=====
SFP 1 Temp High Alarm threshold      = 95.000C
SFP 1 Voltage High Alarm threshold   = 3.900V
SFP 1 Bias High Alarm threshold      = 17.000mA
SFP 1 TX Power High Alarm threshold  = 0.631mW
SFP 1 RX Power High Alarm threshold  = 1.259mW
SFP 1 Temp Low Alarm threshold       = -25.000C
SFP 1 Voltage Low Alarm threshold    = 2.700V
SFP 1 Bias Low Alarm threshold       = 1.000mA
SFP 1 TX Power Low Alarm threshold    = 0.067mW
SFP 1 RX Power Low Alarm threshold    = 0.010mW
=====
SFP 1 Temp High Warning threshold    = 90.000C
SFP 1 Voltage High Warning threshold = 3.700V
SFP 1 Bias High Warning threshold    = 14.000mA
SFP 1 TX Power High Warning threshold = 0.631mW
SFP 1 RX Power High Warning threshold = 0.794mW
SFP 1 Temp Low Warning threshold     = -20.000C
SFP 1 Voltage Low Warning threshold  = 2.900V
SFP 1 Bias Low Warning threshold     = 2.000mA
SFP 1 TX Power Low Warning threshold = 0.079mW
SFP 1 RX Power Low Warning threshold = 0.016mW
=====
SFP 1 Temperature                    = 39.930C
SFP 1 Voltage                        = 3.293V
SFP 1 Tx Bias Current                = 6.894mA
SFP 1 Tx Power                      = 0.328mW
SFP 1 Rx Power                      = 0.000mW
=====
SFP 1 Data Ready state Bar           = False
SFP 1 Rx LOS state                   = True
SFP 1 Tx Fault state                 = False
SFP 1 Rate Select state              = False
SFP 1 RS state                       = False
SFP 1 Tx Disable state               = False
=====
SFP 1 Temperature High Alarm Flag    = False
SFP 1 Voltage High Alarm Flag        = False
SFP 1 Tx Bias High Alarm Flag        = False
SFP 1 Tx Power High Alarm Flag       = False
SFP 1 Rx Power High Alarm Flag       = False
SFP 1 Temperature Low Alarm Flag     = False
SFP 1 Voltage Low Alarm Flag         = False
SFP 1 Tx Bias Low Alarm Flag         = False
SFP 1 Tx Power Low Alarm Flag        = False
SFP 1 Rx Power Low Alarm Flag        = True
=====
!-----output truncated -----!

```

Related Commands

[interface](#) — configures a physical interface on the switch.

[show ip interface](#) — displays Layer 3 information about the interfaces.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

[show inventory](#) — displays the switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.

show range

Display all interfaces configured using the `interface range` command.

Z9500

Syntax `show range`

Command Modes INTERFACE RANGE (config-if-range)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced.

Example

```
Dell(conf-if-range-so-2/0-1,fa-0/0)#show range
interface sonet 2/0 - 1
interface fastethernet 0/0
Dell(conf-if-range-so-2/0-1,fa-0/0)#
```

Related Commands [interface](#) — configures a physical interface on the switch.

[show ip interface](#) — displays Layer 3 information about the interfaces.

[show interfaces](#) — displays information on a specific physical interface or virtual interface.

show running-config ecmp-group

Display interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution using the `ecmp-group monitoring enable` command. The ECMP group could have a LAG or a list of 10G/40 interfaces (not just LAG link-bundles).

Z9500

Syntax `show running-config ecmp-group`

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Related Commands [ecmp-group](#) — configures a mechanism to monitor traffic distribution.

shutdown

Disable an interface.

Z9500

Syntax `shutdown`
To activate an interface, use the `no shutdown` command.

Defaults The interface is disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, enter `no shutdown` on the port channel interface and at least one interface within that port channel.

The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.

Related Commands

[interface port-channel](#) — creates a port channel interface.

[interface vlan](#) — creates a VLAN.

[show ip interface](#) — displays the interface routing status. Add the keyword `brief` to display a table of interfaces and their status.

speed (Management interface)

Set the speed for the Management interface.

Z9500

Syntax

```
speed {10 | 100 | auto}
```

To return to the default setting, use the `no speed {10 | 100}` command.

Parameters

10	Enter the keyword <code>10</code> to set the interface's speed to 10 Mb/s.
100	Enter the keyword <code>100</code> to set the interface's speed to 10/100 Mb/s.
auto	Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed.

Defaults	auto																
Command Modes	INTERFACE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the S55, S60, and S4810</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.11.1	Introduced on the S55, S60, and S4810	8.1.1.0	Introduced on the E-Series ExaScale.	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.11.1	Introduced on the S55, S60, and S4810																
8.1.1.0	Introduced on the E-Series ExaScale.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.0	Introduced on the E-Series.																
Usage Information	This command is found on the Management interface only.																
Related Commands	interface ManagementEthernet — configures the Management port on the system (either the Primary or Standby RPM). management route — configures a static route that points to the Management interface or a forwarding router.																

switchport

Place an interface in Layer 2 mode.

Z9500

Syntax	<pre>switchport [backup interface {tengigabit slot/port fortyGigE slot/port port-channel number}]</pre> To remove an interface from Layer 2 mode and place it in Layer 3 mode, enter the <code>no switchport</code> command. If a switchport backup interface is configured, first remove the backup configuration. To remove a switchport backup interface, enter the <code>no switchport backup interface {tengigabit slot/port fortyGigE slot/port port-channel number}</code> command.	
Parameters	backup interface	Use this option to configure a redundant Layer 2 link without using Spanning Tree. The keywords <code>backup interface</code> configures a backup port so that if the primary port fails, the backup port changes to the up state. If the primary later comes up, it becomes the backup.

	tengigabit Enter the keyword <code>tengigabit</code> if the backup port is a 10G port. fortyGigE Enter the keyword <code>fortyGigE</code> if the backup port is a 40G port. port-channel Enter the keywords <code>port-channel</code> if the backup port is a static or dynamic port channel. slot/port Specify the line card and port number of the backup port.																								
Defaults	Disabled (The interface is in Layer 3 mode.)																								
Command Modes	INTERFACE																								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.4.1.0</td><td>Added support for port-channel interfaces (the <code>port-channel number</code> option).</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.7.1.0</td><td>Added the <code>backup interface</code> option.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.4.1.0	Added support for port-channel interfaces (the <code>port-channel number</code> option).	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.7.1.0	Added the <code>backup interface</code> option.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description																								
9.2(1.0)	Introduced on the Z9500.																								
8.3.19.0	Introduced on the S4820T.																								
8.3.11.1	Introduced on the Z9000.																								
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																								
8.4.1.0	Added support for port-channel interfaces (the <code>port-channel number</code> option).																								
8.3.7.0	Introduced on the S4810.																								
8.1.1.0	Introduced on the E-Series ExaScale.																								
7.7.1.0	Added the <code>backup interface</code> option.																								
7.6.1.0	Introduced on the S-Series.																								
7.5.1.0	Introduced on the C-Series.																								
6.2.1.0	Introduced on the E-Series.																								
Usage Information	If an IP address or VRRP group is assigned to the interface, you cannot use the <code>switchport</code> command on the interface. To use the <code>switchport</code> command on an interface, only the <code>no ip address</code> and <code>no shutdown</code> statements must be listed in the <code>show config</code> output. When you enter the <code>switchport</code> command, the interface is automatically added to the default VLAN. To use the <code>switchport backup interface</code> command on a port, first enter the <code>switchport</code> command. For more information, refer to the "Configuring																								

Redundant Links” section in the “Layer 2” chapter of the *Dell Networking OS Configuration Guide*.

**Related
Commands**

[interface port-channel](#) — creates a port channel interface.

[show interfaces switchport](#) — displays information about switchport interfaces.

Egress Interface Selection (EIS) Commands

The following commands are Egress Interface Selection (EIS) commands.

application

Configure the management egress interface selection.

Z9500

Syntax

`application {all | application-type}`

To remove a management application configuration, use the `no application {all | application-type}` command.

Parameters

application-type

Enter any of the following keywords:

- For DNS, enter the keyword `dns`.
- For FTP, enter the keyword `ftp`.
- For NTP, enter the keyword `ntp`.
- For Radius, enter the keyword `radius`.
- For sFlow collectors, enter the keyword `sflow-collector`.
- For SNMP (traps and MIB responses), enter the keywords `snmp`.
- For SSH, enter the keyword `ssh`.
- For Syslog, enter the keyword `syslog`.
- For TACACS, enter the keyword `tacacs`.
- For Telnet, enter the keyword `telnet`.
- For TFTP, enter the keyword `tftp`.

all

Configure all applications.

Defaults

None.

**Command
Modes**

EIS Mode (conf-mgmt-eis)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

clear management application pkt-cntr

Clear management application packet counters for all management application types.

Z9500

Syntax

```
clear management application pkt-cntr
```

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

clear management application pkt-fallback-cntr

Clear management application packet fallback counters for all management application types.

Z9500

Syntax

```
clear management application pkt-fallback-cntr
```

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

management egress-interface-selection

To make configured application traffic egress through the management port instead of the front-end (FE) port, enable and configure a management egress interface.

Z9500

Syntax	<pre>management egress-interface-selection</pre> To disable and remove management egress interface selection (EIS) configurations, use the <code>no management egress-interface-selection</code> command.
Defaults	None.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

show ip management-eis-route

Display the management routes used by EIS.

Z9500

Syntax	<pre>show ip management-eis-route</pre>
Defaults	None.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show ip management-eis-route
Destination      Gateway          State      Route Source
-----
10.11.0.0/16     ManagementEthernet 0/0    Connected  Connected
172.16.1.0/24   10.11.192.4      Active   Static
```

show management application pkt-cntr

Display the number of packets for each application type that have taken the management route.

Z9500

Syntax `show management application pkt-cntr`

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show management application pkt-cntr
dns          : 2
ftp          : 0
ntp          : 0
radius       : 0
sflow-collector : 0
snmp         : 0
ssh          : 0
syslog       : 0
tacacs       : 0
telnet       : 0
tftp         : 0
```


show management application pkt-fallback-cntr

Display the number of packets for each application type that have been rerouted to the default routing table due to management port or route lookup failure.

Z9500

Syntax `show management application pkt-fallback-cntr`

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show management application pkt-fallback-cntr
dns                : 0
ftp                : 0
ntp                : 0
radius             : 0
sflow-collector    : 0
snmp               : 0
ssh                : 2
syslog             : 0
tacacs             : 0
telnet             : 0
tftp               : 0
```

Port Channel Commands

A Link Aggregation Group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In the Dell Networking OS, a LAG is referred to as a Port Channel.

- For the S-Series, the maximum port channel ID is 128 and the maximum members per port channel is 8.

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed. In the S-Series, stack members can provide those ports.



NOTE: The implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about the link aggregation control protocol (LACP) for dynamic LAGs, refer to the [Link Aggregation Control Protocol \(LACP\)](#) chapter. For more information about configuring and using Port Channels, refer to the *Dell Networking OS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

Z9500

Syntax	<code>channel-member interface</code> To delete an interface from a Port Channel, use the <code>no channel-member interface</code> command.	
Parameters	<i>interface</i>	(OPTIONAL) Enter any of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	Not configured.	
Command Modes	INTERFACE PORTCHANNEL	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the `shutdown`, `description`, `mtu`, and `ip mtu` commands can be configured on an interface if it is added to a Port Channel. The `mtu` and `ip mtu` commands are only available when the chassis is in Jumbo mode.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

Related Commands

[description](#) — assigns a descriptive text string to the interface.

[interface port-channel](#) — creates a Port Channel interface.

[shutdown](#) — disables/enables the port channel.

group

Group two LAGs in a supergroup ("fate-sharing group" or "failover group").

Z9500

Syntax

```
group group_number port-channel number port-channel number
```

To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters

<i>group_number</i>	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
<i>port-channel number</i>	Enter the keywords <code>port-channel</code> then an existing LAG number. Enter this keyword/variable combination twice, identifying the two paired LAGs.

Defaults

none

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Related Commands

[port-channel failover-group](#) — accesses PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

[show interfaces port-channel](#) — displays information on configured Port Channel groups.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing eight physical interfaces on the S-Series.

Z9500

Syntax

```
interface port-channel channel-number
```

To delete a Port Channel, use the `no interface port-channel channel-number` command.

Parameters

<i>channel-number</i>	For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
------------------------------	---

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on S4810.
8.3.11.1	Introduced on Z9000.
8.1.1.0	Introduced on E-Series ExaScale.
7.6.1.0	Introduced on S-Series.
7.5.1.0	Introduced on C-Series.
6.2.1.0	Introduced on E-Series.

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

The `shutdown`, `description`, and `name` commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can only have the `shutdown`, `description`, and `name` commands configured. The Port Channel's configuration is applied to the interfaces within the Port Channel.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, the system determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. For more information, refer to [channel-member](#).

If the line card is in a Jumbo mode chassis, you can also configure the `mtu` and `ip mtu` commands. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.



NOTE: In a Jumbo-enabled system, all members of a Port Channel must be configured with the same link MTU values and the same IP MTU values.

Example

```
Dell(conf)#int port-channel 2
Dell(conf-if-po-2)#
```

Related Commands

[channel-member](#) — adds a physical interface to the LAG.

[interface](#) — configures a physical interface.

[interface loopback](#) — configures a Loopback interface.

[interface null](#) — configures a null interface.

[interface vlan](#) — configures a VLAN.

[shutdown](#) — disables/enables the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

Z9500

Syntax	<code>minimum-links number</code>	
Parameters	number	Enter the number of links in a LAG that must be in “oper up” status. The range is from 1 to 16. The default is 1 .
Defaults	1	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information	If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.
-------------------	---

port-channel failover-group

To configure a LAG failover group, access PORT-CHANNEL FAILOVER-GROUP mode.

Z9500

Syntax	<code>port-channel failover-group</code> To remove all LAG failover groups, use the <code>no port-channel failover-group</code> command.
--------	---

Defaults	none														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.1.1.0	Introduced on the E-Series ExaScale.														
7.6.1.0	Introduced on the S-Series.														
Usage Information	This feature groups two LAGs to work in tandem as a supergroup. For example, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For more information, refer to the "Port Channel" chapter in the <i>Dell Networking OS Configuration Guide</i>.														
Related Command	group — groups two LAGs in a supergroup ("fate-sharing group"). show interfaces port-channel — displays information on configured Port Channel groups.														

show config

Display the current configuration of the selected LAG.

Z9500

Syntax	<code>show config</code>
Command Modes	INTERFACE PORTCHANNEL
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown
Dell(conf-if-po-1)#
```

show interfaces port-channel

Display information on configured Port Channel groups.

Z9500

Syntax

```
show interfaces port-channel [channel-number] [brief]
```

Parameters

channel-number	For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series. Modified to display the LAG failover group status.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show interfaces port-channel` command shown in the following example.

Field	Description
Port-Channel 1...	Displays the LAG's status. In the Example, the status of the LAG's LAG fate-sharing group ("Failover-group") is listed.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Port-channel is part...	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
Members in this...	Displays the interfaces belonging to this port channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the <code>show interfaces</code> counters were cleared.
Queueing strategy.	States the packet queuing strategy. FIFO means first in first out.
packets input...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers, and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.

Field	Description
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

Example

```

Dell#show interfaces port-channel 20
Port-channel 20 is up, line protocol is up (Failover-group 1
is down)
Hardware address is 00:01:e8:01:46:fa
Port-channel is part of failover-group 1
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel: Te 0/5 Te 0/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 00:00:00
Queueing strategy: fifo
  44507301 packets input, 3563070343 bytes
  Input 44506754 IP Packets, 0 Vlans 0 MPLS
  41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-
byte pkts
  407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over
1023-byte pkts
  Received 0 input symbol errors, 0 runts, 0 giants, 0
throttles
  0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
  1218120 packets output, 100745130 bytes, 0 underruns
  Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
  1216142 IP Packets, 0 Vlans, 0 MPLS
  0 throttles, 0 discarded
Rate info (interval 299 sec):
  Input 01.50Mbits/sec, 2433 packets/sec
  Output 00.02Mbits/sec, 4 packets/sec
Time since last interface status change: 00:22:34

Dell#

```

User Information

The following describes the `show interfaces port-channel brief` command shown in the following example.

Field	Description
LAG	Lists the port channel number.
Mode	Lists the mode: • L3 — for Layer 3 • L2 — for Layer 2
Status	Displays the status of the port channel. • down — if the port channel is disabled (shutdown)

Field	Description
	up — if the port channel is enabled (no shutdown)
Uptime	Displays the age of the port channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this port channel.
(untitled)	Displays the status of the physical interfaces (up or down). - In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU. - In Layer 3 port channels, the primary port is not indicated.

Example

```
Dell#sh int por 1 br

LAG Mode Status Uptime    Ports
1   L2   up    00:00:08   Te 2/0   (Up) *
                  Te 2/1   (Down)
                  Te 2/2   (Up)

Dell#
```

Related Commands

[show lacp](#) — displays the LACP matrix.

show port-channel-flow

Display an egress port in a given port-channel flow.

Z9500

Syntax

```
show port-channel-flow outgoing-port-channel number incoming-
interface interface {source-ip address destination-ip address}
| {source-port number destination-port number} | {source-mac
address destination-mac address {vlan vlanid | ether-type}}
```

Parameters

outgoing-port-channel <i>number</i>	Enter the keywords <code>outgoing-port-channel</code> then the number of the port channel to display flow information. For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
incoming-interface <i>interface</i>	Enter the keywords <code>incoming-interface</code> then the interface type and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

source-ip address	Enter the keywords <code>source-ip</code> then the IP source address in IP address format.
destination-ip address	Enter the keywords <code>destination-ip</code> then the IP destination address in IP address format.
source-port number	Enter the keywords <code>source-port</code> then the source port number. The range is from 1 to 65536. The default is None .
destination-port number	Enter the keywords <code>destination-port</code> then the destination port number. The range is from 1 to 65536. The default is None .
source-mac address	Enter the keywords <code>source-mac</code> then the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac address	Enter the keywords <code>destination-mac</code> then the MAC destination address in the nn:nn:nn:nn:nn:nn format.
vlan vlan-id	Enter the keywords <code>vlan</code> then the VLAN-id. The range is from 0 to 4094.
ether-type	Enter the keywords <code>ether-type</code> in the XX:XX format.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Usage Information

Because this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, not for routed packets (use the `show ip flow` command to display routed packets).

The `show port-channel-flow` command returns the egress port identification in a given port-channel if a valid flow is entered. A mismatched flow error occurs if MAC-based hashing is configured for a Layer 2 interface and you are trying to display a Layer 3 flow.

The output displays three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, the egress port of the first fragment.

- In the event of fragmented packets, the egress port of the subsequent fragments.



NOTE: In the `show port channel flow` command output, the egress port for an unknown unicast, multicast, or broadcast traffic is not displayed.

The following example shows the `show port-channel-flow outgoing-port-channel number incoming-interface interface source-mac address destination-mac address`

- Load-balance is configured for MAC
- Load-balance is configured for IP 4-tuple/2-tuple
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address

Example

```
Dell#show port-channel-flow outgoing-port-channel 1 incoming-
interface te 2/0
source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

Egress Port for port-channel 1, for the given flow, is Te
2/1
```

HiGig Port Channel Commands

High-Gigabit Ethernet (HiGig) port channels are used to transmit data between internal backplane ports on line-card (leaf) and switch fabric module (SFM - spine) network processing units (NPUs). You can configure an SNMP trap to be generated when traffic distribution in a HiGig port channel is uneven.



NOTE: HiGig port channels on the backplane are also referred to as *HiGig link bundles* in Z9500 documentation and CLI.

On the Z9500, backplane port channels operate as HiGig link bundles to transmit data traffic between line-card and SFM NPUs. There are 11 line-card and 6 SFM NPUs. The 6 SFM (spine) NPUs comprise the switch fabric module; the 11 line-card (leaf) NPUs are used across three Z9500 line cards.

Line-card NPUs are numbered as follows:

- Line-card slot 0 uses three NPUs numbered 0 to 2.
- Line-card slot 1 uses four NPUs numbered 0 to 3.
- Line-card slot 2 uses four NPUs numbered 0 to 3.

SFM NPUs are numbered 0 to 5.

Line-card and SFM NPUs use HiGig port channels to transmit data.

- An SFM NPU uses 11 HiGig port channels, one port channel to transmit data to each line-card NPU. Each HiGig port channel in an SFM NPU consists of two HiGig links.

- A line-card NPU supports 12 front-end I/O ports and 12 backplane HiGig ports. The 12 backplane links are members of a single HiGig port channel that connects the line-card NPU to each SFM NPU. Two HiGig links in the port channel are used to connect to each SFM NPU.

clear hardware hg-stats

Clear traffic statistics from a HiGig port in a HiGig link bundle/port channel on a line-card or switch fabric module (SFM) NPU.

Z9500

Syntax	<code>clear hardware {sfm <i>npu-id</i> linecard <i>slot</i>} hg-stats {port <i>hg-port-number</i> unit <i>npu-id</i> port <i>hg-port-number</i>}</code>	
Parameters	<i>sfm npu-id</i>	Specify a Z9500 SFM (spine) NPU by entering the keyword <code>sfm</code> and SFM NPU ID. Valid SFM NPU IDs are 0 to 5.
	<i>linecard slot</i>	Specify a Z9500 line-card (leaf) NPU by entering the keyword <code>linecard</code> and line-card slot. Valid slot numbers are 0 to 2.
	<i>hg-stats {port hg-port-number unit npu-id port hg-port-number}</i>	Enter the keyword <code>hg-stats</code> to clear HiGig port statistics. For an SFM NPU HiGig link bundle, specify only a HiGig port number. Valid SFM <i>hg-port-number</i> values are 1 to 22. For a line-card NPU HiGig link bundle, specify an NPU ID and a HiGig port number. Line-card NPUs range from 0 to 3. Line-card HiGig port numbers range from 50 to 61.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Added support for the <code>hg-stats</code> option on the Z9000 platform.

Example

```

Dell# clear hardware linecard 0 hg-stats unit 0 port 59

Dell# show hardware linecard 0 hg-stats unit 0 port 59
Higig Port Statistics:
HiGigabitEthernet 0/0/59,
Input Statistics:
    0 packets, 0 bytes
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
Output Statistics:

```

```

0 packets, 0 bytes 0 underruns
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
0 Multicasts, 0 Broadcasts 0 Unicasts
0 throttles, 0 discarded, 8247266722598448750 collisions
7236269947061497449 wredDrops
Rate info (interval 15 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate

```

Related Commands [show hardware hg-stats](#) — displays traffic statistics from internal ports in a HiGig link bundle.

hg-link-bundle-monitor enable

Enable the monitoring of link utilization and traffic distribution in backplane HiGig link bundles/port channels on a line-card or switch fabric module (SFM) NPU.

Z9500

Syntax `hg-link-bundle-monitor {sfm npu-id hg-port-channel hg-port-channel-id | slot slot npuUnit npu-id hg-port-channel 0} enable`
To disable HiGig link-bundle monitoring, use the `no` version of this command.

Parameters

<code>sfm npu-id hg-port-channel hg-port-channel-id</code>	Specify a HiGig port channel on a Z9500 SFM (spine) NPU by entering the keyword <code>sfm</code> and SFM NPU ID, then <code>hg-port-channel</code> and a HiGig port channel ID. SFM NPU IDs are 0 to 5; SFM HiGig port-channel IDs are 0 to 10.
<code>slot slot-id npuUnit npu-id hg-port-channel 0</code>	Specify a HiGig port channel on a Z9500 line-card (leaf) NPU by entering the keyword <code>slot</code> and slot number, then <code>npuUnit</code> and line-card NPU ID, then <code>hg-port-channel 0</code> . Line-card slot numbers are 0 to 2; line-card NPU IDs are 0 to 3. The HiGig port-channel ID is always 0 because there is only one HiGig link bundle on a line-card NPU.
<code>enable</code>	Enable HiGig link-bundle monitoring.

Command Mode CONFIGURATION

Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 switch.

Usage Information You can configure HiGig link bundle monitoring so that a system log message or an SNMP trap is generated when traffic distribution in a bundle is uneven. The formula that determines uneven traffic distribution is predefined.

hg-link-bundle-monitor rate-interval

Specify the interval (in seconds) for polling traffic distribution in the member links of a HiGig link bundle.

Z9500

Syntax	<code>hg-link-bundle-monitor rate-interval <i>seconds</i></code>	
	To restore the default value, use the <code>no</code> version of this command.	
Parameters	<i>seconds</i>	Polling interval in seconds. The valid values are from 10 to 299.
Command Mode	CONFIGURATION	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 switch.
Defaults	The default polling interval for HiGig link bundles is 15 seconds.	
Usage Information	The rate interval used to poll member links is globally configured and applied to all HiGig link bundles in the system.	

hg-link-bundle-monitor trigger-threshold

Specify the bandwidth-percentage threshold used in HiGig link-bundle monitoring to determine uneven traffic distribution and when an alarm is generated.

Z9500

Syntax	<code>hg-link-bundle-monitor trigger-threshold <i>percentage</i></code>	
	To restore the default value, use the <code>no</code> version of this command.	
Parameters	<i>percentage</i>	Trigger threshold (in percentage of link-bundle bandwidth) at which an SNMP trap is generated. Valid values are 1 to 90.
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 platform.
Defaults	The default trigger-threshold value is 60.	

Usage Information	The trigger-threshold of bandwidth usage, which determines when the calculation of link-bundle utilization is performed, is set at 60 percent of the link-bundle bandwidth. When the total traffic use (mean) is below the trigger-threshold percentage, unevenness in link-bundle traffic distribution is not reported. If traffic unevenness is detected in three consecutive measurements, an alarm is issued. The time interval between measurements is defined by the rate interval for HiGig link polling (default 15 seconds).
--------------------------	---

show hardware hg-stats

Display the traffic statistics from internal ports in a HiGig link bundle/port channel on a line-card or switch fabric module (SFM) NPU.

Z9500

Syntax	<code>show hardware {sfm <i>npu-id</i> linecard <i>slot</i>} hg-stats {port <i>hg-port-number</i> unit <i>npu-id</i> port <i>hg-port-number</i>}</code>	
Parameters	<i>sfm npu-id</i>	Specify a Z9500 SFM (spine) NPU by entering the keyword <code>sfm</code> and SFM NPU ID. Valid SFM NPU IDs are 0 to 5.
	<i>linecard slot</i>	Specify a Z9500 line-card (leaf) NPU by entering the keyword <code>linecard</code> and line-card slot. Valid slot numbers are 0 to 2.
	<i>hg-stats {port hg-port-number unit npu-id port hg-port-number}</i>	Enter the keyword <code>hg-stats</code> to display HiGig port statistics. For an SFM NPU HiGig link bundle, specify only a HiGig port number. Valid SFM <i>hg-port-number</i> values are 1 to 22. For a line-card NPU HiGig link bundle, specify an NPU ID and a HiGig port number. Line-card NPUs range from 0 to 3. Line-card HiGig port numbers range from 50 to 61.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Added support for the <code>hg-stats</code> option on the Z9000 platform.
Example (Line-card HiGig Port)	<pre>Dell# show hardware linecard 0 hg-stats unit 0 port 59 Higig Port Statistics: HiGigabitEthernet 0/0/59, Input Statistics: 0 packets, 0 bytes 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-</pre>	

```

byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  1566541600 packets, 125323328000 bytes 0 underruns
  0 64-byte pkts, 1566541600 over 64-byte pkts, 0 over 127-
byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts 1566541600 Unicasts
  0 throttles, 0 discarded, 0 collisions 0 wredDrops
Rate info (interval 15 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of
line-rate

```

Example (SFM HiGig Port)

```

Dell# show hardware sfm 5 hg-stats port 19
HiGig Port Statistics:
HiGigabitEthernet 3/5/19,
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  63970532045 packets, 5117642582960 bytes 0 underruns
  0 64-byte pkts, 63970531981 over 64-byte pkts, 0 over 127-
byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts 63970532058 Unicasts
  0 throttles, 0 discarded, 0 collisions 0 wredDrops
Rate info (interval 15 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 37096.40 Mbits/sec,    57963128 packets/sec, 94.88%
of line-rate

```

Example (SFM HiGig Port)

```

Dell# show hardware sfm 5 hg-stats port 19
HiGig Port Statistics:
HiGigabitEthernet 3/5/19,
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  63970532045 packets, 5117642582960 bytes 0 underruns
  0 64-byte pkts, 63970531981 over 64-byte pkts, 0 over 127-
byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-
byte pkts
  0 Multicasts, 0 Broadcasts 63970532058 Unicasts
  0 throttles, 0 discarded, 0 collisions 0 wredDrops

```

```

Rate info (interval 15 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of
line-rate
  Output 37096.40 Mbits/sec,    57963128 packets/sec, 94.88%
of line-rate

```

Related Commands [clear hardware hg-stats](#) — clears traffic statistics from internal ports in a HiGig link bundle.

show hg-link-bundle-distribution

Display the operational status and link utilization in a HiGig link bundle.

Z9500

Syntax `show hg-link-bundle-distribution {sfm npu-id hg-port-channel hg-port-channel-id | slot slot npuUnit npu-id hg-port-channel 0} enable`

Parameters

<code>sfm npu-id hg-port-channel hg-port-channel-id</code>	Specify a HiGig port channel on a Z9500 SFM (spine) NPU by entering the keyword <code>sfm</code> and SFM NPU ID, then <code>hg-port-channel</code> and a HiGig port channel ID. SFM NPU IDs are 0 to 5; SFM HiGig port-channel IDs are 0 to 10.
<code>slot slot-id npuUnit npu-id hg-port-channel 0</code>	Specify a HiGig port channel on a Z9500 line-card (leaf) NPU by entering the keyword <code>slot</code> and slot number, then <code>npuUnit</code> and NPU ID, then <code>hg-port-channel 0</code> . Line-card slot numbers are 0 to 2; line-card NPU IDs are 0 to 3. The HiGig port-channel ID is always 0 because there is only one HiGig link bundle used on a line-card NPU to connect to SFM NPUs.

Command Modes EXEC, EXEC Privilege

Command History	Version	Description
	9.2.(1.0)	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 switch.

Usage Information The following table illustrates the fields displayed in the output of this command:

Field	Description
Link-bundle trigger threshold	Percentage value of link-bundle bandwidth that serves as the threshold for marking a link bundle as being overutilized, triggering link-bundle monitoring, and generating an SNMP alarm.
Slot	Slot number of a Z9500 line card.

Field	Description
npuUnit	Network processing unit (NPU) ID number of a HiGig link bundle/port-channel.
hg-port-channel	Port-channel number of a HiGig link bundle.
Utilization (In Percent)	Percentage of total bandwidth usage by the traffic transmitted on the HiGig link bundle.
Alarm State	Indicates whether an alarm has been generated if uneven traffic distribution occurs in a HiGig link bundle. Possible values are Active and Inactive.
Interface	Member interface of the specified HiGig link bundle/port channel in the format: <i>slot-id/npu-id:hghigig-port-number</i>
Utilization (In Percent)	Percentage of total link-bundle bandwidth used on each member link.

Example

```
Dell# show hg-link-bundle-distribution slot 0 npuUnit 2 hg-
port-channel 0

hg-link-bundle trigger threshold - 60
Slot 0 npuUnit 2 hg-port-channel-0 Utilization [In Percent] -
0 Alarm State - Inactive
Interface Utilization [In Percent]
0/2:hg0          10
0/2:hg1          10
0/2:hg2          10
0/2:hg3          10
```

snmp-server enable traps hg-lbm

Enable the generation of SNMP traps and notifications when HiGig link-bundle monitoring is enabled.

Z9500

Syntax

```
snmp-server enable traps hg-lbm
```

Parameters

hg-lbm Enter the keyword `hg-lbm` to enable traps for HiGig link-bundle monitoring.

Command Modes

CONFIGURATION mode

Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 platform.

UDP Broadcast

The user datagram protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

Important Points to Remember

- Routing information protocol (RIP) is not supported with the UDP Broadcast feature.
- If you configure this feature on an interface using the `ip udp-helper udp-port` command, the `ip directed-broadcast` command becomes ineffective on that interface.
- The existing `show interface` command has been modified to display the configured broadcast address.

debug ip udp-helper

Enable UDP debug and display the debug information on a console.

Z9500

Syntax	<pre>debug ip udp-helper</pre> To disable debug information, use the <code>no debug ip udp-helper</code> command.												
Defaults	Debug disabled.												
Command Modes	• EXEC • EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the E-Series ExaScale.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.7.0	Introduced on the E-Series ExaScale.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
8.3.7.0	Introduced on the E-Series ExaScale.												

Example

```
Dell#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Te 1/0 with IP DA (0xffffffff) will be
sent on Te 1/1 Gi 1/2
Vlan 3

01:44:54: Pkt rcvd on Te 2/0 is handed over for DHCP
processing.
```

Related Commands

[ip udp-helper udp-port](#) — enables the UDP broadcast feature on an interface.

[show ip udp-helper](#) — displays the configured UDP helper(s) on all interfaces.

ip udp-helper udp-port

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Z9500

Syntax

```
ip udp-helper udp-port [udp-port-list]
```

To disable the UDP broadcast on a port, use the `no ip udp-helper udp-port [udp-port-list]` command.

Parameters

udp-port-list (OPTIONAL) Enter up to 16 comma-separated UDP port numbers.

 **NOTE:** If you do not use this option, all UDP ports are considered by default.

Defaults none

Command Modes INTERFACE (config-if)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.7.0	Introduced on the E-Series ExaScale.

Usage Information

If you configure the `ip helper-address` command and `ip udp-helper udp-port` command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server per the `ip helper-address` configuration. This occurs regardless if the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If you only configure the `ip udp-helper udp-port` command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

Related Commands

[ip helper-address](#) — configures the destination broadcast or host address for the DHCP server.

[debug ip udp-helper](#) — enables debug and displays the debug information on a console.

[show ip udp-helper](#) — displays the configured UDP helpers on all interfaces.

show ip udp-helper

Display the configured UDP helpers on all interfaces.

Z9500

Syntax

```
show ip udp-helper
```

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.7.0	Introduced on the E-Series ExaScale.

Example

```
Dell#show ip udp-helper
-----
Port      UDP  port  list
-----
```

```
Te 1/0 656, 658
Te 1/1 All
```

Related Commands

[debug ip udp-helper](#) — enables debug and displays the debug information on a console.

[ip udp-helper udp-port](#) — enables the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Internet Protocol Security (IPSec)

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — Connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — Confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — Algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes: Transport and Tunnel.

- Transport is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- Tunnel mode is used to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating virtual private networks (VPNs).

Transport mode provides IP packet payload protection using ESP. You can use ESP alone or in combination with AH to provide additional authentication. AH protects data from modification but does not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. The SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.



NOTE:

Due to performance limitations on the control processor, you cannot enable IPSec on all packets in a communication session.

crypto ipsec transform-set

Create a transform set, or combination of security algorithms and protocols, of cryptos.

Z9500

Syntax

```
crypto ipsec transform-set name {ah-authentication {md5|sha1|
null} | esp-authentication {md5|sha1|null} | esp-encryption
{3des|cbc|des|null}}
```

To delete a transform set, use the `no crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}` command.

Parameters

<i>name</i>	Enter the name for the transform set.
ah-authentication	Enter the keywords <code>ah-authentication</code> then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • <code>md5</code> — Use Message Digest 5 (MD5) authentication. • <code>sha1</code> — Use Secure Hash Algorithm 1 (SHA-1) authentication. • <code>null</code> — Causes an encryption policy configured for the area to not be inherited on the interface.
esp-authentication	Enter the keywords <code>esp-authentication</code> then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • <code>md5</code> — Use Message Digest 5 (MD5) authentication. • <code>sha1</code> — Use Secure Hash Algorithm 1 (SHA-1) authentication. • <code>null</code> — Causes an encryption policy configured for the area to not be inherited on the interface.
esp-encryption	Enter the keywords <code>esp-encryption</code> then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. • <code>3des</code> — Use 3DES encryption. • <code>cbc</code> — Use CDC encryption. • <code>des</code> — Use DES encryption. • <code>null</code> — Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.
Version	Description						
9.2(1.0)	Introduced on the Z9500.						
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.						
Usage Information	- Both sides of the link must specify the same transform set. - You can create up to 64 transform sets.						
Example	<pre>Dell(conf)#int ten 0/4 Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64 Dell(conf)#int ten 0/6 Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64</pre>						

crypto ipsec policy

Create a crypto policy used by ipsec.

Z9500

Syntax	<pre>crypto ipsec policy name seq-num ipsec-manual</pre> To delete a crypto policy entry, use the <code>no crypto ipsec policy name seq-num ipsec-manual</code> command.						
Parameters	<table> <tr> <td>name</td><td>Enter the name for the crypto policy set.</td></tr> <tr> <td>seq-num</td><td>Enter the sequence number assigned to the crypto policy entry.</td></tr> </table>	name	Enter the name for the crypto policy set.	seq-num	Enter the sequence number assigned to the crypto policy entry.		
name	Enter the name for the crypto policy set.						
seq-num	Enter the sequence number assigned to the crypto policy entry.						
Defaults	none						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.
Version	Description						
9.2(1.0)	Introduced on the Z9500.						
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.						
Usage Information	This command creates a crypto policy entry and enters the crypto policy configuration mode for configuring the flow parameters.						

Example

```
Dell(conf)#crypto ipsec policy West 10 ipsec-manual
Dell(conf-crypto-policy)#
```

management crypto-policy

Apply the crypto policy to management traffic.

Z9500

Syntax

```
management crypto-policy name
```

To remove the management traffic crypto policy, use the `no management crypto-policy name` command.

Parameters

name Enter the name for the crypto policy..

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

match

Apply an match filter to the crypto policy.

Z9500

Syntax

```
match seq-num tcp [source ip address | ipv6 address {mask}
{source-port number}] [destination ip address | ipv6 address
{mask} {destination-port number}]
```

To remove the match filter for the crypto map, use the `no match seq-num tcp [source ip address | ipv6 address {mask} {source-port number}] [destination ip address | ipv6 address {mask} {destination-port number}]` command.

Parameters	seq-num	Enter the match command sequence number.
	sourceip-address ipv6 address	Enter the keyword <code>source</code> then the IPv4 or IPv6 address for the source.
	mask	Enter the mask prefix length in /nn format.
	source-port number	Enter the source port number.
	destination-port number	Enter the destination port number.

Defaults none

Command Modes CONFIG-CRYPTO-POLICY

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

- Usage Information**
- IPv4 addresses support only -/32 mask types.
 - IPv6 addresses support only -/128 mask types.
 - Configure match for bi-directional traffic for optimal routing.
 - Only TCP is supported.

Example

```
match 0 tcp a::1 /128 0 a::2 /128 23
match 1 tcp a::1 /128 23 a::2 /128 0
match 2 tcp a::1 /128 0 a::2 /128 21
match 3 tcp a::1 /128 21 a::2 /128 0
match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32 23
match 5 tcp 1.1.1.1 /32 23 1.1.1.2 /32 0
match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32 21
match 7 tcp 1.1.1.1 /32 21 1.1.1.2 /32 0
```

session-key

Specify the session keys used in the crypto policy entry.

Z9500

Syntax `session-key {inbound | outbound} {ah spi hex-key-string | esp spi encrypt hex-key-string auth hex-key-string}`

To delete the session key information from the crypto policy, use the `no session-key {inbound | outbound} {ah | esp}` command.

Parameters	<i>name</i>	Enter the name for the transform set.
	<i>inbound</i>	Specify the inbound session key for IPSec.
	<i>outbound</i>	Specify the outbound session key for IPSec.
	<i>ah</i>	Use the AH protocol when you select the AH transform set in the crypto policy.
	<i>esp</i>	Use the ESP protocol when you select the ESP transform set in the crypto policy.
	<i>spi</i>	Enter the security parameter index number.
	<i>hex-key-string</i>	Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.
	<i>encrypt</i>	Indicates the ESP encryption transform set key string.
	<i>auth</i>	Indicates the ESP authentication transform set key string.

Defaults none

Command Modes CONF-CRYPTO-POLICY

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

- Usage Information**
- This command is only available in the ipsec-manual model.
 - The key information entry is associated with the global method for enabling clear text or encrypted display in the running config.

show crypto ipsec transform-set

Display the transform set configuration.

Z9500

Syntax `show crypto ipsec transform-set name`

Parameters

<i>name</i>	Enter the name of the transform set.
-------------	--------------------------------------

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show crypto ipsec transform-set

Transform-Set Name      : dallas
Transform-Set refCnt    : 0
AH Transform            :
ESP Auth Transform      :
ESP Encry Transform     : 3des
Dell#
```

show crypto ipsec policy

Display the crypto policy configuration.

Z9500

Syntax `show crypto ipsec policy`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show crypto ipsec policy

Policy name           : West
Policy refcount       : 1
Sequence Num          : 10
SA Mode               : IPSEC-MANUAL
Transform-Set Name    : dallas
Peer IP Address       :
Inbound AH SPI        : 0
Inbound ESP Auth SPI  : 0
Inbound ESP Encry SPI : 256
Inbound AH Key        : [0]::
Inbound ESP Auth Key  : [0]::
Inbound ESP Encry Key :
[96]::a5b6b42009d47895b420a5b6789509d4b420a5b6789509d4b420a5b67
89509d4b420a5b6789509d4b420a5b6789509d4
Outbound AH SPI       : 0
Outbound ESP Auth SPI : 0
Outbound ESP Encry SPI : 257
Outbound AH Key       : [0]::
Outbound ESP Auth Key : [0]::
Outbound ESP Encry Key :
[96]::a5b6b42009d47895b420a5b6789509d4b420a5b6789509d4b420a5b67
89509d4b420a5b6789509d4b420a5b6789509d4

Match sequence Num    : 0
Protocol type         : tcp
IP or IPv6            : IPv6
Source address        : a::1
Source mask           : /128
Source port           : 0
Destination address   : a::2
Destination mask      : /128
Destination port      : 23
source-interface name :
source-interface num  :

Match sequence Num    : 1
Protocol type         : tcp
IP or IPv6            : IPv6
Source address        : a::1
Source mask           : /128
Source port           : 23
Destination address   : a::2
Destination mask      : /128
Destination port      : 0
source-interface name :
source-interface num  :

Match sequence Num    : 2
Protocol type         : tcp
IP or IPv6            : IPv6
Source address        : a::1
Source mask           : /128
Source port           : 0
```



```

Destination address : a::2
Destination mask    : /128
Destination port    : 21
source-interface name :
source-interface num :

```

```

Match sequence Num : 3
Protocol type       : tcp
IP or IPv6          : IPv6
Source address      : a::1
Source mask         : /128
Source port         : 21
Destination address : a::2
Destination mask    : /128
Destination port    : 0
source-interface name :
source-interface num :

```

Dell#

transform-set

Specify the transform set the crypto policy uses.

Z9500

Syntax

```
transform-set transform-set-name
```

To delete a transform set from the crypto policy, use the `no transform-set transform-set-name` command.

Parameters

transform-set-name Enter the name for the crypto policy transform set.

Defaults

none

Command

CONFIG-CRYPTO-POLICY

Modes

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

IPv4 Routing

The basic IPv4 commands are supported by Dell Networking operating system on the switch.

arp

To associate an IP address with a MAC address in the switch, use address resolution protocol (ARP).

Z9500

Syntax	<code>arp ip-address mac-address interface</code> To remove an ARP address, use the <code>no arp ip-address</code> command.	
Parameters	<i>ip-address</i>	Enter an IP address in dotted decimal format.
	<i>mac-address</i>	Enter a MAC address in nnnn.nnnn.nnnn format.
	<i>interface</i>	(OPTIONAL) Enter any of the following keywords and slot/port or number information: • For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
	8.3.7.0	Introduced on the S4810.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.2.1.0	Introduced on the E-Series.
Usage Information	You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.	
Related Commands	clear arp-cache — clears dynamic ARP entries from the ARP table. show arp — displays the ARP table.	

arp backoff-time

Set the exponential timer for resending unresolved ARPs.

Z9500

Syntax	<code>arp backoff-time seconds</code>	
Parameters	seconds	Enter the number of seconds an ARP entry is black-holed. The range is from 1 to 3600. The default is 30 .
Defaults	30	
Command Mode	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.8.0	Introduced on the S4810.
Usage Information	This timer is an exponential backoff timer. Over the specified period, the time between ARP requests increases. This behavior reduces the potential for the system to slow down while waiting for a multitude of ARP responses.	
Related Commands	show arp retries — displays the configured number of ARP retries.	

arp learn-enable

Enable ARP learning using gratuitous ARP.

Z9500

Syntax	<code>arp learn-enable</code>
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Z9500

Syntax	arp retries <i>number</i>													
Parameters	<i>number</i>	Enter the number of retries. The range is from 5 to 20. The default is 5 .												
Defaults	5													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.1.0</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.1.0	Introduced.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
8.3.1.0	Introduced.													
Usage Information	Retries are 20 seconds apart.													
Related Commands	show arp retries — displays the configured number of ARP retries.													

arp timeout

Set the time interval for an ARP entry to remain in the ARP cache.

Z9500

Syntax	<code>arp timeout minutes</code>	
Parameters	seconds	Enter the number of minutes. The range is from 0 to 35790. The default is 240 minutes .

Defaults	240 minutes (4 hours)																		
Command Modes	INTERFACE																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.2.1.1	Introduced on the E-Series.																		
Related Commands	show interfaces — displays the ARP timeout value for all available interfaces.																		

clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (`no-refresh`) ARP entries from the content addressable memory (CAM).

Z9500

Syntax	<code>clear arp-cache [interface ip ip-address] [no-refresh]</code>	
Parameters	interface	(OPTIONAL) Enter the following keywords and slot/port or number information: - For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

ip *ip-address* (OPTIONAL) Enter the keyword `ip` then the IP address of the ARP entry you wish to clear.

no-refresh (OPTIONAL) Enter the keywords `no-refresh` to delete the ARP entry from CAM. Or use this option with *interface* or `ip ip-address` to specify which dynamic ARP entries you want to delete.



NOTE: Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

clear host

Remove one or all dynamically learned host table entries.

Z9500

Syntax	<code>clear host name</code>	
Parameters	name	Enter the name of the host to delete. Enter * to delete all host table entries.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

clear ip fib linecard

Clear all FIB entries on a Z9500 line card (use this command with caution; refer to *Usage Information*.)

Z9500

Syntax	<code>clear ip fib linecard slot-id</code>	
Parameters	linecard slot-id	Enter the slot ID of a Z9500 line card. Valid slot IDs are from 0 to 2.
Command Modes	EXEC	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.19.0	Introduced on the S4820T.

Usage Information

To clear Layer 3 CAM inconsistencies, use this command.



CAUTION: Executing this command causes traffic disruption.

Related Commands

[show ip fib linecard](#) — shows FIB entries on a specified stack-unit.

clear ip route

Clear one or all routes in the routing table.

Z9500

Syntax

```
clear ip route { * | ip-address mask }
```

Parameters

*	Enter an asterisk (*) to clear all learned IP routes.
ip-address mask	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

- [ip route](#) — assigns an IP route to the switch.
- [show ip route](#) — views the routing table.
- [show ip route summary](#) — views a summary of the routing table.

clear ip traffic

Clear IP traffic statistics on Z9500 CPUs.

Z9500

Syntax

```
clear ip traffic {cp | rp}
```

Parameters

- cp** Clear ip traffic statistics on the Control Processor CPU.
- rp** Clear ip traffic statistics on the Route Processor CPU.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.2.1.1	Introduced on the E-Series.

Related Commands [show ip traffic](#) — displays IP traffic statistics.

clear tcp statistics

Clear TCP counters.

Z9500

Syntax `clear tcp statistics [all | cp | rp]`

Parameters

all	Enter the keyword <code>all</code> to clear TCP statistics maintained on all switch processors.
cp	(OPTIONAL) Enter the <code>cp</code> to clear TCP statistics only from the Control Processor.
rp	(OPTIONAL) Enter the keyword <code>rp1</code> to clear TCP statistics only from the Route Processor.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands [show tcp statistics](#) — displays TCP traffic statistics.

debug arp

View information on ARP transactions.

Z9500

Syntax	<code>debug arp [interface] [count value]</code> To stop debugging ARP transactions, use the <code>no debug arp</code> command.	
Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: - For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>count value</i>	(OPTIONAL) Enter the keyword <code>count</code> then the count value. The range is from 1 to 65534.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the <code>count</code> option.

Usage Information To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip dhcp

Enable debug information for dynamic host configuration protocol (DHCP) relay transactions and display the information on the console.

Z9500

Syntax `debug ip dhcp`
To disable debug, use the `no debug ip dhcp` command.

Defaults Debug disabled

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.10	Introduced on the E-Series.

Example

```
Dell#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr =
```

```

00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, teaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received
at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr =
00:60:CF:20:7B:8C, teaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for
00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at
interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:
8C, teaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for
00:60:CF:20:7B:8C to 113.3.3.254
Dell#

```

Related Commands

[ip helper-address](#) – specifies the destination broadcast or host address for the DHCP server request.

[ip helper-address hop-count disable](#) – disables the hop-count increment for the DHCP relay agent.

debug ip icmp

View information on the internal control message protocol (ICMP).

Z9500

Syntax

```
debug ip icmp [interface] [count value]
```

To disable debugging, use the `no debug ip icmp` command.

Parameters

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a Tunnel interface, enter the keywords `tunnel` then a number. The range is from 1 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

count value (OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is **Infinity**.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the <code>count</code> option.

Example

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

**Usage
Information**

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip packet

View a log of IP packets sent and received.

Z9500

Syntax

```
debug ip packet [access-group name] [count value] [interface]
```

To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface]` command.

Parameters

**access-group
name**

Enter the keyword `access-group` then the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.

count value

(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is `Infinity`.

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. For the C-Series and S-Series, the range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Command
Modes**

EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Added the <code>access-group</code> option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the <code>count</code> option.

Usage Information

The following describes the `debug ip packet` command in the following example.

Field	Description
s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.
len	Displays the packet's length.
sending, rcvd, fragment, sending broad/multicast proto, unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of the original datagram.

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739,
    win=8191 ACK PUSH
```

```

IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226,
sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739,
win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500,
sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 2/11), len 64,
sending broad/multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 2/11), len 28,
sending broad/multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
    ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
    ICMP type=8, code=0

```

Usage Information

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

The `access-group` option supports only the equal to (`eq`) operator in TCP ACL rules. Port operators not equal to (`neq`), greater than (`gt`), less than (`lt`), or range are not supported in `access-group` option (refer to the following example). ARP packets (`arp`) and Ether-type (`ether-type`) are also not supported in the `access-group` option. The entire rule is skipped to compose the filter.

The `access-group` option pertains to:

- IP protocol number: from 0 to 255
- Internet control message protocol (`icmp`) but not the ICMP message type (from 0 to 255)
- Any internet protocol (`ip`)
- Transmission Control Protocol (`tcp`) but not on the `rst`, `syn`, or `urg` bits
- User Datagram Protocol (`udp`)

In the case of ambiguous access control list rules, the `debug ip packet access-control` command is disabled. A message appears identifying the error (refer to the Example below).

Example (Error Messages)

```

Dell#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

Dell#00:10:45: %RPM0-P:CP
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not
supported in access-list debug, access-list debugging is

```

```
turned off
Dell#
```

ip address

Assign a primary and secondary IP address to the interface.

Z9500

Syntax

```
ip address {ip-address mask [secondary] | dhcp}
```

To delete an IP address from an interface, use the `no ip address [ip-address]` command.

Parameters

<i>ip-address</i>	Enter an IP address in dotted decimal format.
<i>mask</i>	Enter the mask of the IP address in slash prefix format (for example, /24).
<i>secondary</i>	(OPTIONAL) Enter the keyword <code>secondary</code> to designate the IP address as the secondary address.
<i>dhcp</i>	Enter the keyword <code>dhcp</code> to configure an interface to receive its IP address from the configured DHCP server.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information	You must be in INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering ROUTER OSPF mode.
--------------------------	---

ip directed-broadcast

Enables the interface to receive directed broadcast packets.

Z9500

Syntax	<code>ip directed-broadcast</code> To disable the interface from receiving directed broadcast packets, use the <code>no ip directed-broadcast</code> command.
Defaults	Disabled (that is, the interface does not receive directed broadcast packets)
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

ip domain-list

Configure names to complete unqualified host names.

Z9500

Syntax	<code>ip domain-list name</code> To remove the name, use the <code>no ip domain-list name</code> command.
---------------	--

Parameters	<i>name</i> Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).																
Defaults	Disabled.																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.1.1.0	Introduced on the E-Series ExaScale.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
Usage Information	To configure a list of possible domain names, configure the <code>ip domain-list</code> command up to six times. If you configure both the <code>ip domain-name</code> and <code>ip domain-list</code> commands, the software tries to resolve the name using the <code>ip domain-name</code> command. If the name is not resolved, the software goes through the list of names configured with the <code>ip domain-list</code> command to find a match. To enable dynamic resolution of hosts, use the following steps: • specify a domain name server with the <code>ip name-server</code> command • enable DNS with the <code>ip domain-lookup</code> command To view current bindings, use the <code>show hosts</code> command. To view a DNS-related configuration, use the <code>show running-config resolve</code> command.																
Related Commands	ip domain-name — specifies a DNS server.																

ip domain-lookup

To address resolution (that is, DNS), enable dynamic host-name.

Z9500

Syntax	<code>ip domain-lookup</code> To disable DNS lookup, use the <code>no ip domain-lookup</code> command.																
Defaults	Disabled.																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
8.1.1.0	Introduced on the E-Series ExaScale.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
Usage Information	To fully enable DNS, also specify one or more domain name servers with the <code>ip name-server</code> command. The system does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port. To view current bindings, use the <code>show hosts</code> command.																
Related Commands	ip name-server — specifies a DNS server. show hosts — Views the current bindings.																

ip domain-name

Configure one domain name for the switch.

Z9500

Syntax	<code>ip domain-name name</code> To remove the domain name, use the <code>no ip domain-name</code> command.																	
Parameters	name	Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).																
Defaults	Not configured.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
8.1.1.0	Introduced on the E-Series ExaScale.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
Usage Information	You can only configure one domain name with the <code>ip domain-name</code> command. To configure more than one domain name, configure the <code>ip domain-list</code> command up to six times. To enable dynamic resolution of hosts, use the following steps: • specify a domain name server with the <code>ip name-server</code> command • enable DNS with the <code>ip domain-lookup</code> command To view current bindings, use the <code>show hosts</code> command.																	
Related Commands	ip domain-list — configures additional names.																	

ip helper-address

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

Z9500

Syntax `ip helper-address ip-address`
To remove a DHCP server address, use the `no ip helper-address` command.

Parameters *ip-address* Enter an IP address in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

The system uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and the system forwards to the client with source port=67, destination port=68.

ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

Z9500

Syntax `ip helper-address hop-count disable`
To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.

Defaults Enabled; the hops field in the DHCP message header is incremented by default.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced for the E-Series.

Usage Information This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through the system. If the incoming boot request already has a non-zero hops field, the message is relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

Related Commands [ip helper-address](#) — specifies the destination broadcast or host address for DHCP server requests.

[show running-config](#) — displays the current configuration and changes from the default values.

ip host

Assign a name and IP address the host-to-IP address mapping table uses.

Z9500

Syntax	<code>ip host name ip-address</code> To remove an IP host, use the <code>no ip host name [ip-address]</code> command.	
Parameters	name	Enter a text string to associate with one IP address.
	ip address	Enter an IP address, in dotted decimal format, to be mapped to the name.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced for the E-Series.

ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

Z9500

Syntax	<code>ip max-frag-count count</code> To place no limit on the number of fragments allowed, use the <code>no ip max-frag-count</code> command.																			
Parameters	count	Enter a number for the number of fragments allowed for re-assembly. The range is from 2 to 256.																		
Defaults	No limit is set on number of fragments allowed.																			
Command Modes	CONFIGURATION																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced for the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced for the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
8.1.1.0	Introduced on the E-Series ExaScale.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.0	Introduced for the E-Series.																			
Usage Information	To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.																			

ip mtu

Set the IP MTU (frame size) of the packet the RPM transmits for the line card interface. If the packet must be fragmented, the system sets the size of the fragmented packets to the size specified in this command.

Z9500

Syntax	<code>ip mtu value</code> To return to the default IP MTU value, use the <code>no ip mtu</code> command.													
Parameters	value	Enter the maximum MTU size if the IP packet is fragmented. The range is from 576 to 9234. The default is 1500 bytes .												
Defaults	1500 bytes													
Command Modes	INTERFACE													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	6.1.1.0	Introduced on the E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.7.0	Introduced on the S4810.													
8.1.1.0	Introduced on the E-Series ExaScale.													
6.1.1.0	Introduced on the E-Series.													
Usage Information	When you enter the <code>no mtu</code> command, the system reduces the <code>ip mtu</code> value to 1536 bytes. To return the IP MTU value to the default, use the <code>no ip mtu</code> command. Compensate for Layer 2 header when configuring link MTU on an Ethernet interface or the system may not fragment packets. If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (the <code>ip mtu</code> command) must be enough bytes to include for the Layer 2 header. Link MTU and IP MTU considerations for Port Channels and VLANs are as follows Port Channels: • All members must have the same link MTU value and the same IP MTU value. • The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.													

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following describes the difference between Link MTU and IP MTU.

Layer 2 Overhead	Difference between Link MTU and IP MTU
Ethernet (untagged)	18 bytes
VLAN Tag	Tag 22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

Related Commands

[mtu](#) — sets the link MTU for an Ethernet interface.

ip name-server

Enter up to six IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

Z9500

Syntax

```
ip name-server ipv4-address [ipv4-address2...ipv4-address6]
```

To remove a name server, use the `no ip name-server ip-address` command.

Parameters

<i>ipv4-address</i>	Enter the IPv4 address, in dotted decimal format, of the name server to be used.
<i>ipv4-address2...ipv4-address6</i>	(OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults

No name servers are configured.

Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.1.1.0	Introduced on the E-Series.																		
Usage Information	The system does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port. You can separately configure both IPv4 and IPv6 domain name servers.																		
Related Commands	ipv6 name-server — configures an IPv6 name server.																		

ip proxy-arp

Enable proxy ARP on an interface.

Z9500

Syntax	<pre>ip proxy-arp</pre> To disable proxy ARP, use the <code>no ip proxy-arp</code> command.
Defaults	Enabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands [show ip interface](#) — displays the interface routing status and configuration.

ip route

Assign a static route to the switch.

Z9500

Syntax `ip route {destination mask {ip-address | interface [slot/port] | [tunnel tunnel-id] [distance] | [permanent] | tag tag-value}}`

To delete a specific static route, use the `no ip route destination mask` command.

To delete all routes matching a certain route, use the `no ip route destination mask` command.

Parameters

<i>destination</i>	Enter the IP address in dotted decimal format of the destination device.
<i>mask</i>	Enter the mask in the slash prefix format (/x) of the destination IP address.
<i>ip-address</i>	Enter the IP address of the forwarding router in dotted decimal format.
interface <i>slot/port</i>	Enter the keyword <code>interface</code> then the slot/port number.
tunnel <i>tunnel-id</i>	Enter the keyword <code>tunnel</code> then the tunnel ID.
<i>distance</i>	(OPTIONAL) Enter the value of the distance metric assigned to the route. The range is from 1 to 255.

permanent	(OPTIONAL) Enter the keyword <code>permanent</code> to specify that the route must not be removed even if the interface assigned to that route goes down. The route must be currently active to be installed in the routing table. If you disable the interface, the route is removed from the routing table.
tag tag-value	(OPTIONAL) Enter the keyword <code>tag</code> then a number to assign to the route. The range is from 1 to 4294967295.
bfd	Enter the keyword <code>bfd</code> to use bidirectional forwarding detection.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for tunnel interface type.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Using the following example of a static route: `ip route 33.33.33.0 /24 tengigabitethernet 0/0 172.31.5.43`

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if `te 0/0` has an ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, the system installs the static route.
- When the interface goes down, the system withdraws the route.
- When the interface comes up, the system re-installs the route.

- When recursive resolution is “broken,” the system withdraws the route.
- When recursive resolution is satisfied, the system re-installs the route.

**Related
Commands**

[show ip route](#) — views the switch routing table.
[show ipv6 route](#) — displays the IPv6 routes.

ip source-route

Enable the system to forward IP packets with source route information in the header.

Z9500

Syntax

`ip source-route`

To drop packets with source route information, use the `no ip route-source` command.

Defaults

Enabled.

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ip unreachable

Enable the generation of internet control message protocol (ICMP) unreachable messages.

Z9500

Syntax	<code>ip unreachable</code> To disable the generation of ICMP messages, use the <code>no ip unreachable</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ipv4 unicast-host-route

Enable the storage of IPv4 route prefixes in the L3 host table.

Z9500

Syntax	<code>[no] ipv4 unicast-host-route</code>
Defaults	Disabled; by default, all IPv4 route prefixes are stored installed only in the Longest Prefix Match (LPM) table.
Command Modes	CONFIGURATION

Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.3(0.1)	Introduced on the S6000.
Usage Information	Route prefixes stored in the L3 host table are managed using ECMP next-hop forwarding.	
	A warning message is displayed after you enter the command stating that this setting takes effect for existing routes only when IPv4 route prefixes are cleared from the LPM routing table (RTM). To enable storage of IPv4 route prefixes in the LPM table, disable this setting by entering the <code>no ipv4 unicast-host-route</code> command.	
Example	<pre> Dell(conf)#ipv4 unicast-host-route Warning: Command will take effect for existing routes only when IPv4 route prefixes are cleared from RTM Dell(conf)#no ipv4 unicast-host-route </pre>	

load-balance

By default, the system uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the `load-balance` command.

Z9500

Syntax	<pre>load-balance {ip-selection [dest-ip source-ip]} {mac [dest-mac source-dest-mac source-mac]} {tcp-udp ingress-port [enable]}</pre> To return to the default setting (IP 4-tuple), use the <code>no load-balance {ip-selection [dest-ip source-ip]} {mac [dest-mac source-dest-mac source-mac]} {tcp-udp ingress-port [enable]}</code> command.
---------------	---

Parameters	ip-selection {dest-ip source-ip}	Enter the keywords to distribute IP traffic based on the following criteria:
		<code>dest-ip</code> — Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. <code>source-ip</code> — Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

mac {dest-mac source-dest-mac source-mac}	Enter the keywords to distribute MAC traffic based on the following criteria: • dest-mac — Uses the destination MAC address, VLAN, EtherType, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. • source-dest-mac — Uses the destination and source MAC address, VLAN, EtherType, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded. • source-mac — Uses the source MAC address, VLAN, EtherType, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
tcp-udp enable	Enter the keywords to distribute traffic based on the following: • enable — Takes the TCP/UDP source and destination ports into consideration when doing hash computations. This option is enabled by default.
ingress-port enable	Enter the keywords to distribute traffic based on the following: • enable — Takes the source port into consideration when doing hash computations. This option is disabled by default.

Defaults

IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Added the <code>ingress-port</code> parameter for the S4810.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

**Usage
Information**

By default, the system distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address
- TCP/UDP source port
- TCP/UDP destination port

**Related
Commands**

[hash-algorithm ecmp](#) — changes the hash algorithm across an ECMP.

load-balance hg

Choose the traffic flow parameters the hash calculation uses while distributing the traffic across internal hlgig links.

Z9500

Syntax

```
[no] load-balance hg { ip-selection | ipv6-selection [source-ip  
| source-ipv6 | source-port-id | source-module-id | dest-ip |  
dest-ipv6 | dest-port-id | dest-module-id | protocol | vlan |  
L4-source-port | L4-dest-port ] | mac [source-mac | source-  
port-id | source-module-id | dest-mac | dest-port-id | dest-  
module-id | vlan | ethertype | source-dest-mac ] | tunnel  
[ipv4-over-ipv4 | ipv4-over-gre-ipv4 | mac-in-mac]}
```

Parameters

**{ip-selection|
ipv6-selection
[source-ip |
source-ipv6 |
source-port-id
| source-
module-id |
dest-ip | dest-
ipv6 | dest-
port-id | dest-
module-id |
protocol | vlan |
L4-source-port
| L4-dest-port]**

To use IPv4 key fields in hash computation, enter the keyword `ip-selection` then one of the parameters. To use IPv6 key fields in hash computation, enter the keyword `ipv6-selection` then one of the parameters.

- `source-ip` — Use IPv4 src-ip field in hash calculation.
- `source-ipv6` — Use IPv6 src-ip field in hash calculation
- `source-port-id` — Use src-port-id field in hash calculation.
- `source-module-id` — Use src-module-id field in hash calculation.
- `dest-ip` — Use IPv4 dest-ip field in hash calculation.
- `dest-ipv6` — Use IPv6 dest-ip field in hash calculation
- `dest-port-id` — Use dest-port-id field in hash calculation.
- `dest-module-id` — Use dest-module-id field in hash calculation.
- `protocol` — Use IPv4 protocol field in hash calculation.
- `vlan` — Use vlan field in hash calculation.
- `L4-source-port` — Use IPv4 L4-source-port field in hash calculation.

- L4-dest-port — Use IPv4 L4-dest-port field in hash calculation.

mac [*source-mac* | *source-port-id* | *source-module-id* | *dest-mac* | *dest-port-id* | *dest-module-id* | *vlan* | *ethertype* | *source-dest-mac*]

To use MAC key fields in hash computation, enter the keyword **mac** then one of the parameters:

- *source-mac* — Use *source-mac* field in hash calculation.
- *source-port-id* — Use *src-port-id* field in hash calculation.
- *source-module-id* — Use *src-module-id* field in hash calculation.
- *dest-mac* — Use *dest-mac* field in hash calculation.
- *dest-port-id* — Use *dest-port-id* field in hash calculation.
- *dest-module-id* — Use *dest-module-id* field in hash calculation.
- *vlan* — Use *vlan* field in hash calculation .
- *ethertype* — Use *Ethertype* field in hash calculation.
- *source-dest-mac* — Use *SMAC* and *DMAC* fields in hash calculation.

tunnel [*ipv4-over-ipv4* | *ipv4-over-gre-ipv4* | *mac-in-mac*]}

To use tunnel key fields in hash computation, enter the keyword **tunnel** then one of the parameters:

- *ipv4-over-ipv4* — Use *ipv4-over-ipv4* field in hash calculation.
- *ipv4-over-gre-ipv4* — Use *ipv4-over-gre-ipv4* field in hash calculation.
- *mac-in-mac* — Use *mac-in-mac* field in hash calculation.

Defaults

IP selection 5-tuples (source-ip dest-ip vlan protocol L4-source-port L4-dest-port).

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

management route

Configure a static route that points to the Management interface or a forwarding router.

Z9500

Syntax

```
management route {{ip-address mask | {ipv6-address prefix-length}} {forwarding-router-address | managementethernet}
```

To remove a static route, use the `no management route{{ip-address mask | {ipv6-address prefix-length}}{forwarding-router-address | managementethernet}` command.

Parameters	<i>ip-address mask</i>	Enter an IP address (dotted decimal format) and mask (/prefix format) of the destination subnet.
	<i>ipv6-address prefix-length</i>	Enter an IPv6 address (x:x:x:x::x format) and mask (/prefix format) of the destination subnet. Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is from /0 to /128.
	<i>forwarding-router-address</i>	Enter an IP address (dotted decimal format) or an IPv6 address (x:x:x:x::x format) of a forwarding router.
	<i>managementethernet</i>	Enter the keyword <code>managementethernet</code> for the Management interface on the Primary RPM.

 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000 and added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.

	Version	Description
	6.1.1.0	Introduced on the E-Series.
Usage Information	When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.	
Related Commands	interface ManagementEthernet — configures the Management port on the system (either the Primary or Standby RPM). duplex (Management) — sets the mode of the Management interface. speed (Management interface) — sets the speed for the Management interface.	

show arp

Display the ARP entries learned on a Z9500 CPU.

Z9500

Syntax	<pre>show arp [cpu [cp rp]] [interface <i>interface</i> ip <i>ip-address</i> [<i>mask</i>] macaddress <i>mac-address mask</i>] [static dynamic] [summary]</pre>	
Parameters	cpu cp	(OPTIONAL) Enter the keywords <code>cpu cp</code> to display the ARP entries learned on the Control Processor.
	cpu rp	(OPTIONAL) Enter the keyword <code>cpu rp</code> to display the ARP entries learned on the Route Processor.
	interface <i>interface</i>	To specify an interface, enter one of the following interface types and slot/port or number information: • For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a tunnel interface, enter the keyword <code>tunnel</code>.

linecard slot-id	(OPTIONAL) Enter the <i>interface port-type slot/port</i> parameters to display the ARP entries learned on a Z9500 port. The range of slot IDs is from 0 to 2.
ip ip-address mask	(OPTIONAL) Enter the keyword <i>ip</i> with an IP address in the dotted decimal format to display the ARP entries learned with this IP address. Enter the optional IP address mask in the slash prefix format (/ x).
macaddress mac-address mask	(OPTIONAL) Enter the keyword <i>macaddress</i> with a MAC address in nn:nn:nn:nn:nn:nn format to display the ARP entries learned with this MAC address. Enter the optional MAC address mask in nn:nn:nn:nn:nn:nn format also.
static	(OPTIONAL) Enter the keyword <i>static</i> to display manually-entered ARP entries.
dynamic	(OPTIONAL) Enter the keyword <i>dynamic</i> to display dynamically-learned ARP entries.
summary	(OPTIONAL) Enter the keyword <i>summary</i> to view a summary of ARP entries.

Default

Display only the ARP entries learned on the Control Processor.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.8.1.0	Augmented to display local ARP entries learned from private VLANs (PVLANS).
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

Usage Information

Use the `show arp` command to display the ARP entries learned on the Control Processor and Route Processor.

The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to [Private VLAN \(PVLAN\)](#)).

The following describes the `show arp` command shown in the following example.

Row Heading	Description
Protocol	Displays the protocol type.
Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age (in minutes) of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

Example

```
Dell>show arp
```

Protocol	Address	Age(min)	Hardware Address	Interface	VLAN	CPU
Internet	192.2.1.254	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.253	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.252	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.251	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.250	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.251	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.250	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.249	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.248	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.247	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.246	1	00:00:c0:02:01:02	Te 0/13	-	CP
Internet	192.2.1.245	1	00:00:c0:02:01:02	Te 0/13	-	CP

Example (Private VLAN)



NOTE: In this example, Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN. Line 2 shows primary VLAN 10.

```
Dell#show arp
```

Protocol	Address	Age(min)	Hardware Address	Interface	VLAN	CPU
Internet	5.5.5.1	-	00:01:e8:43:96:5e	-	Vl 10	pv
200	CP					
Internet	5.5.5.10	-	00:01:e8:44:99:55	-	Vl	
10	CP					
Internet	10.1.2.4	1	00:01:e8:d5:9e:e2	Ma 0/0		
-	CP					
Internet	10.10.10.4	1	00:01:e8:d5:9e:e2	Ma 0/0		
-	CP					

```

Internet 10.16.127.53 1 00:01:e8:d5:9e:e2 Ma 0/0
- CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2 Ma 0/0
- CP
Internet 133.33.33.4 1 00:01:e8:d5:9e:e2 Ma 0/0
- CP

```

Usage Information

The following describes the `show arp summary` command shown in the following example.

Row Heading	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.
CPU	Lists which CPU the entries are stored on.

Example (Summary)

```

#show arp summary

TotalEntries Static Entries Dynamic Entries CPU
-----
83            0              83          CP
Dell

```

Related Commands

[ip local-proxy-arp](#) — enables/disables Layer 3 communication in secondary VLANs.

[switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

show arp retries

Display the configured number of ARP retries.

Z9500

Syntax

```
show arp retries
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced.

Related Commands [arp retries](#) — sets the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

View the host table and DNS configuration.

Z9500

Syntax `show hosts`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Added support for IPv6 addresses.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show hosts` command in the following example.

Field	Description
Default domain...	Displays the domain name (if configured).

Field	Description
Name/address lookup...	States if DNS is enabled on the system. - If DNS is enabled, the Name/Address lookup is domain service. - If DNS is not enabled, the Name/Address lookup is static mapping
Name servers are...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: - perm — the entry was manually configured and will not time out - temp — the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route: - ok — the entry is valid. - ex — the entry expired. ?? — the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learned entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP addresses assigned to the host.

Example

```

Dell#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host      Flags      TTL  Type  Address
-----
ks        (perm, OK) -    IP    2.2.2.2
4200-1    (perm, OK) -    IP    192.68.69.2
1230-3    (perm, OK) -    IP    192.68.99.2
ZZr       (perm, OK) -    IP    192.71.18.2
Z10-3     (perm, OK) -    IP    192.71.23.1
Dell#

```

Related Commands

[traceroute](#) — views the DNS resolution.

[ip host](#) — configures a host.

show ip cam linecard

View CAM entries for a port pipe on a line card.

Z9500

Syntax `show ip cam linecard slot-id port-set pipe-number [ip-address mask [longer-prefix] | ecmp-group [details | member-info] | summary]`

Parameters	<i>slot-id</i>	Enter the slot ID of the line card. The range of Z9500 slot IDs is from 0 to 2.
	<i>pipe-number</i>	Enter the number of a line card's port-pipe. The range is from 0 to 3.
	<i>ip-address mask [longer-prefix]</i>	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keyword <i>longer-prefixes</i> to view routes with a common prefix.
	<i>ecmp-group {details member-info}</i>	(OPTIONAL) Enter the keyword <i>ecmp-group</i> and specify if you want to display detailed CAM information about an ECMP group or about individual ECMP-group member ports.
	<i>summary</i>	(OPTIONAL) Enter the keyword <i>summary</i> to view a table listing route prefixes and the total number of routes that can be entered into the CAM.

- Command Modes**
- EXEC
 - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Introduced on the E-Series ExaScale E600i.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip cam` command shown in the following example.

Field	Description
Index	Displays the CAM index number of the entry.
Destination	Displays the destination route of the index.
EC	Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. For Jumbo line cards, displays 0,1 when ECMP is more than eight.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 if the entry is for a line card with Catalog number beginning with LC-EF.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
Next-Hop	Displays the next hop IP address of the entry.
VId	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17c1 CP, the CP is the pertinent portion. • CP = control processor • RP2 = route processor 2 • Te = 10-Gigabit Ethernet interface • Fo = 40-Gigabit Ethernet interface

Example

```
Dell#show ip cam linecard 1 port-set 0
Index  Destination EC CG V C  Next-Hop  VId Mac-Addr  Port
-----
3276   6.6.6.2      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c1 CP
3277   5.5.5.2      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c1 CP
3278   4.4.4.2      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c1 CP
3279   3.3.3.2      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c1 CP
3280   2.2.2.2      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c1 CP
11144   6.6.6.0      0 0 1 1   0.0.0.0  6 00:00:00:00:00:00 17c5 RP2
11145   5.5.5.0      0 0 1 1   0.0.0.0  5 00:00:00:00:00:00 17c5 RP2
11146   4.4.4.0      0 0 1 1   0.0.0.0  4 00:00:00:00:00:00 17c5 RP2
11147   3.3.3.0      0 0 1 1   0.0.0.0  3 00:00:00:00:00:00 17c5 RP2
11148   2.2.2.0      0 0 1 1   0.0.0.0  2 00:00:00:00:00:00 17c5 RP2
65535   0.0.0.0      0 0 1 1   0.0.0.0  0 00:00:00:00:00:00 17c5 RP2
Dell#
```

Usage Information

The following describes the `show ip cam summary` command shown in the following example.

Field	Description
Prefix Length	Displays the prefix-length or mask for the IP address configured on the linecard 0 port pipe 0.
Current Use	Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port pipe 0.
Initial Size	Displays the CAM size allocated for the corresponding mask. The system adjusts the CAM size if the number of routes for the mask exceeds the initial allocation.

**Example
(Summary)**

```
Dell#show ip cam linecard 2 port-set 0 summary
Total Number of Routes in the CAM is 13
Total Number of Routes which can be entered in CAM is 131072
```

Prefix Len	Current Use	Initial Sz
32	7	37994
31	0	1312
30	0	3932
29	0	1312
28	0	1312
27	0	1312
26	0	1312
25	0	1312
24	6	40610
23	0	3932
22	0	2622
21	0	2622
20	0	2622
19	0	2622
18	0	1312
17	0	1312
16	0	3932
15	0	1312
14	0	1312
13	0	1312
12	0	1312
11	0	1312
10	0	1312
9	0	1312
8	0	1312
7	0	1312
6	0	1312
5	0	1312
4	0	1312
3	0	1312
2	0	1312
1	0	1312
0	0	8

Dell#

show ip fib linecard

View all forwarding information base (FIB) entries.

Z9500

Syntax `show ip fib linecard slot-id [ip-address/prefix-list | summary]`

Parameters

slot-id	Enter the slot ID of the line card. The range of Z9500 slot IDs is from 0 to 2.
ip-address mask	(OPTIONAL) Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). Enter the mask in slash prefix format (/X).
longer-prefixes	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view the total number of prefixes in the FIB.

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

**Usage
Information**

The following describes the `show ip fib` command shown in the following example.

Field	Description
Destination	Lists the destination IP address.

Field	Description
Gateway	Displays either the word "direct" and an interface for a directly connected route or the remote IP address used to forward the traffic.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.
Vld	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
Index	Displays the internal interface number.
EC	Displays the number of ECMP paths.

Example

```
Dell>show ip fib linecard 2
```

```

Destination      Gateway                First-Hop    Mac-Addr
Port    Vld Index EC
-----
3.0.0.0/8        via 100.10.10.10, So 2/8 100.10.10.10
00:01:e8:00:03:ff So 2/8 0 60260 0
3.0.0.0/8        via 101.10.10.10, So 2/9
00.10.10.0/24    Direct, So 2/8 0.0.0.0
00:01:e8:00:03:ff So 2/8 0 11144 0
100.10.10.1/32   via 127.0.0.1 127.0.0.1
00:00:00:00:00:00 CP      0 3276 0
100.10.10.10/32 via 100.10.10.10, So 2/8 100.10.10.10
00:01:e8:00:03:ff So 2/8 0 0 0
101.10.10.0/24   Direct, So 2/9 0.0.0.0
00:00:00:00:00:00 RP2     0 11145 0
101.10.10.1/32   via 127.0.0.1 127.0.0.1
00:00:00:00:00:00 CP      0 3277 0
101.10.10.10/32 via 101.10.10.10, So 2/9 101.10.10.10
00:01:e8:01:62:32 So 2/9 0 1 0
Dell>
```

Related Commands

[clear ip fib linecard](#) — clears the FIB entries on a specified line card.

show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

Z9500

Syntax

```
show ip flow interface interface {source-ip address
destination-ip address} {protocol number [tcp | udp]} {src-port
number destination-port number}
```

Parameters	interface <i>interface</i>	Enter the keyword <i>interface</i> then one of the following interface keywords. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.																						
	source-ip <i>address</i>	Enter the keywords <code>source-ip</code> then the IP source address in IP address format.																						
	destination-ip <i>address</i>	Enter the keywords <code>destination-ip</code> then the IP destination address in IP address format.																						
	protocol <i>number</i> [tcp udp]	Enter the keyword <code>protocol</code> then one of the protocol type keywords: <code>tcp</code> , <code>udp</code> , or <code>protocol number</code> The protocol number range is from 0 to 255. .																						
	src-port <i>number</i>	Enter the keywords <code>src-port</code> then the source port number.																						
	destination-port <i>number</i>	Enter the keywords <code>destination-port</code> then the destination port number.																						
Command Modes	EXEC																							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.10.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.9.1.0</td><td>Introduced VRF on the E-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.10.0	Introduced on the S4810.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.1.1.0	Introduced on the E-Series ExaScale.	7.9.1.0	Introduced VRF on the E-Series.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																							
9.2(1.0)	Introduced on the Z9500.																							
8.3.19.0	Introduced on the S4820T.																							
8.3.11.1	Introduced on the Z9000.																							
8.3.10.0	Introduced on the S4810.																							
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																							
8.1.1.0	Introduced on the E-Series ExaScale.																							
7.9.1.0	Introduced VRF on the E-Series.																							
7.6.1.0	Introduced on the S-Series.																							
7.5.1.0	Introduced on the C-Series.																							
6.1.1.0	Introduced on the E-Series.																							
Usage Information	This command provides egress port information for a given IP flow. This information is useful in identifying which interface the packet follows in the case of																							

Port-channel and Equal Cost Multi Paths. Use this command for routed packets only. For switched packets, use the `show port-channel-flow` command.

The `show ip flow` command does not compute the egress port information when `load-balance mac hashing` is also configured due to insufficient information (the egress MAC is not available).

S-Series produces the following error message: %Error: Unable to read IP route table.

Example

```
Dell#show ip flow interface Te 1/8 189.1.1.1 63.0.0.1 protocol
tcp source-port 7898 destination-port 8
```

flow: 189.1.1.1 63.0.0.1 protocol 6 7868 8976

Ingress interface:Te 1/20

Egress interface:Te 1/14 to 1.7.1.2[CAM hit 103710]

unfragmented packet

Te 1/10 to 1.2.1.2[CAM hit 103710] fragmented packet

show ip interface

View IP-related information on all interfaces.

Z9500

Syntax

```
show ip interface [interface | brief] [linecard slot-id]
[configured]
```

Parameters

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `Loopback` then a number from 0 to 16383.
- For the Management interface, enter the keyword `ManagementEthernet` then zero (0).
- For the Null interface, enter the keyword `null` then zero (0).
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

linecard <i>slot-id</i>	Enter the <code>linecard slot-id</code> parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a brief summary of the interfaces and whether an IP address is assigned.
configured	(OPTIONAL) Enter the keyword <code>configured</code> to display the physical interfaces with non-default configurations only.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Supported on the E-Series ExaScale E600i.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip interface` command shown in the following example.

Lines	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port, and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the configured incoming access list. If none is configured, the phrase "not set" is displayed.

Lines	Description
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface.
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachable...	States if ICMP unreachable messages are sent.

Example

```

Dell# show ip interface tengigabitethernet 2
TenGigabitEthernet 2/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

TenGigabitEthernet 2/1 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

TenGigabitEthernet 2/2 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

TenGigabitEthernet 2/3 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
--More--

Dell# show ip interface brief
Interface          IP-Address      OK  Method
Status             Protocol
TenGigabitEthernet 0/0    unassigned      NO  Manual
administratively down
TenGigabitEthernet 0/1    10.10.10.1      NO  Manual
administratively down

```

```

TenGigabitEthernet 0/2    unassigned      NO   Manual
administratively down down
TenGigabitEthernet 0/3    unassigned      NO   Manual
administratively down down
fortyGigE 0/4             unassigned      NO   Manual
administratively down down
fortyGigE 0/8             unassigned      NO   Manual
administratively down down
--More--

Dell# show ip interface configured
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachable are not sent

TenGigabitEthernet 0/1 is down, line protocol is down
Internet address is 10.10.10.1/24
Broadcast address is 10.10.10.255
Address determined by config file
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachable are not sent
--More--

```

Usage Information

The following describes the `show ip interface brief` command shown in the following example.

Fields	Description
Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
OK?	Indicates if the hardware is functioning properly.
Method	Displays "Manual" if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

Example (Brief)

```

Dell#show ip int brief
Interface          IP-Address  OK?  Method
Status            Protocol
TenGigabitEthernet 1/0    unassigned NO   Manual
administratively down down
TenGigabitEthernet 1/1    unassigned NO   Manual
administratively down down

```

```
TenGigabitEthernet 1/2  unassigned  YES Manual
up
TenGigabitEthernet 1/3  unassigned  YES Manual
up
TenGigabitEthernet 1/4  unassigned  YES Manual
up
TenGigabitEthernet 1/5  10.10.10.1  YES Manual
up
TenGigabitEthernet 1/6  unassigned  NO   Manual
administratively down down
```

show ip management-route

View the IP addresses assigned to the Management interface.

Z9500

Syntax	<code>show ip management-route [all connected summary static]</code>	
Parameters	all	(OPTIONAL) Enter the keyword <code>all</code> to view all IP addresses assigned to all Management interfaces on the switch.
	connected	(OPTIONAL) Enter the keyword <code>connected</code> to view only routes directly connected to the Management interface.
	summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing the number of active and non-active routes and their sources.
	static	(OPTIONAL) Enter the keyword <code>static</code> to view non-active routes also.
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip management-route
```

Destination	Gateway	State
-----	-----	-----
10.1.2.0/24	ManagementEthernet 0/0	Connected
172.16.1.0/24	10.1.2.4	Active
Dell#		

show ipv6 management-route

Display the IPv6 static routes configured for the management interface.

Z9500

Syntax

```
show ipv6 management-route [all | connected | summary | static]
```

Parameters

all	(OPTIONAL) Enter the keyword <code>all</code> to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword <code>connected</code> to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword <code>static</code> to view non-active routes also.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.4.1.0	Introduced on the C- and E-Series.

Version	Description
8.3.7.0	Introduced on the S4810.

Example

```
Dell#show ipv6 management-route
IPv6 Destination    Gateway                State
-----
2001:34::0/64      ManagementEthernet 0/0  Connected
2001:68::0/64      2001:34::16          Active
Dell#
```

show ip protocols

View information on all routing protocols enabled and active on the switch.

Z9500

Syntax `show ip protocols`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Regular evaluation optimization enabled/disabled added to display output.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip protocols
Routing Protocol is "bgp 1"
  Cluster Id is set to 20.20.20.3
  Router Id is set to 20.20.20.3
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
```

```

Capable of ROUTE_REFRESH
For Address Family IPv4 Unicast
BGP table version is 0, main routing table version 0
Distance: external 20 internal 200 local 200
Neighbor(s):
  Address : 20.20.20.2
  Filter-list in : foo
  Route-map in : foo
  Weight : 0
  Address : 5::6
  Weight : 0
Dell#

```

show ip route

View information, including how they were learned, about the IP routes on the switch.

Z9500

Syntax

```

show ip route hostname | ip-address [mask] [longer-prefixes] |
list prefix-list | protocol [process-id | routing-tag] | all |
connected | static | summary

```

Parameters

<i>ip-address</i>	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
<i>mask</i>	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
<i>longer-prefixes</i>	(OPTIONAL) Enter the keywords <i>longer-prefixes</i> to view all routes with a common prefix.
list <i>prefix-list</i>	(OPTIONAL) Enter the keyword <i>list</i> and the name of a configured prefix list. For more information, refer to the show ip route list command.
<i>protocol</i>	(OPTIONAL) Enter the name of a routing protocol (<i>bgp</i> , <i>isis</i> , <i>ospf</i> , <i>rip</i>) or the keywords <i>connected</i> or <i>static</i> .



NOTE: *bgp*, *isis*, *ospf*, and *rip*.

- If you enter *bgp*, you can include the BGP *as-number*.
- If you enter *isis*, you can include the ISIS *routing-tag*.
- If you enter *ospf*, you can include the OSPF *process-id*.

<i>process-id</i>	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
<i>routing-tag</i>	(OPTIONAL) Specify that only ISIS routes with a certain routing tag must be displayed.

connected	(OPTIONAL) Enter the keyword <code>connected</code> to view only the directly connected routes.
all	(OPTIONAL) Enter the keyword <code>all</code> to view both active and non-active routes.
static	(OPTIONAL) Enter the keyword <code>static</code> to view only routes the <code>ip route</code> command configures.
summary	(OPTIONAL) Enter the keyword <code>summary</code> . For more information, refer to the show ip route summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip route all` command in the following example.

Field	Description
(undefined)	Identifies the type of route: • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated

Field	Description
	• O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IP address
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
Dell#show ip route all

Codes:C- connected, S - static, R - RIP
      B- BGP, IN - internal BGP, EX - external BGP, LO -
Locally Originated
      O- OSPF, IA - OSPF inter area N1 - OSPF NSSA external
type 1
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
default
      >- non-active route + - summary route

Gateway of last resort is not set

      Destination      Gateway      Dist/Metric  Last Change
-----
R    3.0.0.0/8         via 100.10.10.10, So 2/8 120/1    00:07:12
      via 101.10.10.10, So 2/9
      100.10.10.0/24    Direct, Te 2/8          0/0      00:08:54
> R  100.10.10.0/24    Direct, Te 2/8          120/0     00:08:54
C    101.10.10.0/24    Direct, Te 2/9          0/0      00:09:15
> R  101.10.10.0/24    Direct, Te 2/9          120/0     00:09:15
Dell#
```

Example (Summary)

```
Dell#show ip route summary

Route Source  Active Routes  Non-active Routes
connected     2              0
static        1              0
Total         3              0
```

Total 3 active route(s) using 612 bytes

```
Dell#show ip route static
Destination      Gateway          Dist/Metric Last Change
-----
*S  0.0.0.0/0    via 10.10.91.9, Te 1/2  1/0          3d2h
```

show ip route list

Display IP routes in an IP prefix list.

Z9500

Syntax `show ip route list prefix-list`

Parameters

<i>prefix-list</i>	Enter the name of a configured prefix list.
--------------------	---

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example `Dell#show ip route list test`

```
Codes:C- connected, S - static, R - RIP,
      B- BGP, IN - internal BGP, EX - external BGP, LO -
Locally Originated,
      O- OSPF, IA - OSPF inter area, N1 - OSPF NSSA external
type 1,
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1,
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate
```

```

default,
>- non-active route, + - summary route

Gateway of last resort is not set

      Destination      Gateway             Dist/Metric  Last Change
      -----
R      2.1.0.0/24        via 2.1.4.1, Te 2/43    120/2        3d0h
R      2.1.1.0/24        via 2.1.4.1, Te 2/43    120/2        3d1h
R      2.1.2.0/24        via 2.1.4.1, Te 2/43    120/1        3d0h
R      2.1.3.0/24        via 2.1.4.1, Te 2/43    120/1        3d1h
C      2.1.4.0/24        Direct, Te 2/43         0/0         3d1h

```

Related Commands [ip prefix-list](#) — enters CONFIGURATION-IP PREFIX-LIST mode and configures a prefix list.

[show ip prefix-list summary](#) — displays a summary of the configured prefix lists.

show ip route summary

View a table summarizing the IP routes in the switch.

Z9500

Syntax `show ip route summary`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip route summary` shown in the following example.

Column Heading	Description
Route Source	Identifies how the route is configured in the system.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route becomes the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active...	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the system, this line does not appear.

Example

```
Dell>show ip route summary

Route Source    Active Routes    Non-active Routes
connected       17               0
static          3               0
ospf 100        1368            2
Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total           1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Dell>
```

Related Commands

[show ip route](#) — displays information about the routes found in the switch.

show ip traffic

View IP traffic statistics on Z9500 CPUs, including ICMP, UDP, TCP and ARP counters.

Z9500

Syntax

```
show ip traffic {all | cp | rp}
```

Parameters

all	(OPTIONAL) Enter the keyword <code>all</code> to view IP traffic statistics from all processors.
cp	(OPTIONAL) Enter the keyword <code>cp</code> to view only IP traffic statistics from the Control Processor.
rp	(OPTIONAL) Enter the keyword <code>rp</code> to view only IP traffic statistics from the Route Processor.

Default	View IP traffic statistics from all processors.																				
Command Modes	EXEC Privilege																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.		
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.1.1.0	Introduced on the E-Series.																				
Usage Information	The following describes the <code>show ip traffic</code> summary shown in the following example. <table> <tr> <th>Keyword</th><th>Definition</th></tr> <tr> <td>unknown protocol...</td><td>No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.</td></tr> <tr> <td>not a gateway...</td><td>Packets can not be routed; the host/network is unreachable.</td></tr> <tr> <td>security failures...</td><td>Counts the number of received unicast/multicast packets that could not be forwarded due to: - route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group - destination IP address belongs to reserved prefixes; the host/network is unreachable </td></tr> <tr> <td>bad options...</td><td>Unrecognized IP option on a received packet.</td></tr> <tr> <td>Frag:</td><td>IP fragments received.</td></tr> <tr> <td>... reassembled</td><td>Number of IP fragments that were reassembled.</td></tr> <tr> <td>... timeouts</td><td>Number of times a timer expired on a reassembled queue.</td></tr> <tr> <td>... too big</td><td>Number of invalid IP fragments received.</td></tr> <tr> <td>... couldn't fragment</td><td>Number of packets that could not be fragmented and forwarded.</td></tr> </table>	Keyword	Definition	unknown protocol...	No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.	not a gateway...	Packets can not be routed; the host/network is unreachable.	security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: - route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group - destination IP address belongs to reserved prefixes; the host/network is unreachable	bad options...	Unrecognized IP option on a received packet.	Frag:	IP fragments received.	... reassembled	Number of IP fragments that were reassembled.	... timeouts	Number of times a timer expired on a reassembled queue.	... too big	Number of invalid IP fragments received.	... couldn't fragment	Number of packets that could not be fragmented and forwarded.
Keyword	Definition																				
unknown protocol...	No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.																				
not a gateway...	Packets can not be routed; the host/network is unreachable.																				
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: - route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group - destination IP address belongs to reserved prefixes; the host/network is unreachable																				
bad options...	Unrecognized IP option on a received packet.																				
Frag:	IP fragments received.																				
... reassembled	Number of IP fragments that were reassembled.																				
... timeouts	Number of times a timer expired on a reassembled queue.																				
... too big	Number of invalid IP fragments received.																				
... couldn't fragment	Number of packets that could not be fragmented and forwarded.																				

Keyword	Definition
...encapsulation failed	Counts packets which could not be forwarded due to ARP resolution failure. The system sends an ARP request prior to forwarding an IP packet. If a reply is not received, the system repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	Total number of packets received from specified protocol.
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.
...socket full	The applications buffer is full and the incoming packet are dropped.

The F10 Monitoring MIB provides access to the following statistics.

- **IP Statistics: Bcast: Received:** Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent:** Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received:** Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent:** Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request:** Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies:** Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request:** Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies:** Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy:** Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

Example

```
Dell#show ip traffic
Control Processor IP Traffic:

IP statistics:
  Rcvd: 23857 total, 23829 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
        0 fragmented, 0 couldn't fragment
  Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
  Sent: 16048 generated, 0 forwarded
        21 encapsulation failed, 0 no route
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0
  unreachable
        0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0
```

```

quench
  0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
  0 mask requests, 0 mask replies, 0 quench, 0 timestamp
  0 info reply, 0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  0 short packets, 0 bad length, 0 no port broadcasts, 0
socket full
  Sent: 0 total, 0 forwarded broadcasts
TCP statistics:
  Rcvd: 23829 total, 0 checksum errors, 0 no port
  Sent: 16048 total
ARP statistics:
  Rcvd: 156 requests, 11 replies
  Sent: 21 requests, 10 replies (0 proxy)

```

Related Commands [clear ip traffic](#) — clears IP traffic statistics.

show tcp statistics

Display statistical information about TCP traffic transmitted on Z9500 CPUs.

Z9500

Syntax	show tcp statistics {all cp rp}	
Parameters	all	Enter the keyword <code>all</code> to view all TCP statistics on Z9500 CPUs.
	cp	Enter the keyword <code>cp</code> to view TCP statistics only from the Control Processor.
	rp	Enter the keyword <code>rp1</code> to view TCP statistics only from the Route Processor.
Command Modes	EXEC Privilege	
Default	Display TCP information from all processors.	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.4.1.0	Introduced

Usage Information

The following describes the `show tcp statistics cp` command shown in the following example.

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the switch. - Total = total packets received - no port = number of packets received with no designated port
0 checksum error...	Displays the number of packets received with the following: - checksum errors - bad offset to data - too short
329 packets...	Displays the number of packets and bytes received in sequence.
17 dup...	Displays the number of duplicate packets and bytes received.
0 partially...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the switch's window size.
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack...	Displays the number of acknowledgement packets and bytes received.
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.

Field	Description
25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack..	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
7 Connections initiated...	Displays the number of TCP connections initiated, accepted, and established.
14 Connections closed...	Displays the number of TCP connections closed, dropped.
20 Total rxmt...	Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive....	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

Example

```
Dell#show tcp statistics cp

Control Processor TCP:
Rcvd: 10585 Total, 0 no port
    0 checksum error, 0 bad offset, 0 too short
    329 packets (1263 bytes) in sequence
    17 dup packets (6 bytes)
    0 partially dup packets (0 bytes)
    7 out-of-order packets (0 bytes)
    0 packets ( 0 bytes) with data after window
    0 packets after close
    0 window probe packets, 41 window update packets
    41 dup ack packets, 0 ack packets with unsend data
    10184 ack packets (12439508 bytes)
Sent: 12007 Total, 0 urgent packets
    25 control packets (including 24 retransmitted)
    11603 data packets (12439677 bytes)
    24 data packets (7638 bytes) retransmitted
    355 ack only packets (41 delayed)
    0 window probe packets, 0 window update packets
    7 Connections initiated, 8 connections accepted, 15
connections established
    14 Connections closed (including 0 dropped, 0 embryonic
dropped)
    20 Total rxmt timeout, 0 connections dropped in rxmt timeout
    0 Keepalive timeout, 0 keepalive probe, 0 Connections
dropped in keepalive
Dell#
```

**Related
Commands**

[clear tcp statistics](#) — clears TCP traffic statistics.

IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking operating system.

 **NOTE:** For IPv4 ACL commands, refer to the [Access Control Lists \(ACL\)](#) chapter.

Important Points to Remember

- Certain platforms require manual CAM usage space allotment. For more information, refer to the [cam-acl](#) command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.

cam-acl

Allocate space for IPv6 ACLs.

Z9500

Syntax `cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10}`

Parameters

default

Use the default CAM profile settings, and set the CAM as follows:

- L3 ACL (ipv4acl): **6**
- L2 ACL(l2acl): **5**
- IPv6 L3 ACL (ipv6acl): **0**
- L3 QoS (ipv4qos): **1**
- L2 QoS (l2qos): **1**

	l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10	Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The <code>ipv6acl</code> range must be a factor of 2.
--	---	---

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.2.0	Introduced on the E-Series TeraScale.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information For the new settings to take effect, save the new CAM settings to the startup-config (`write mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

cam-acl-egress

Allocate space for IPv6 egress ACLs.

Z9500

Syntax `cam-acl-egress {default | l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}`

Parameters **default** Use the default CAM profile settings, and set the CAM as follows:

- L2 ACL(l2acl): **1**
- L3 ACL (ipv4acl): **1**
- IPv6 L3 ACL (ipv6acl): **2**

l2acl 1-4
ipv4acl 1- 4
ipv6acl 0-4

Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 2.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.2.0	Introduced on the E-Series TeraScale.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

Example

```
Dell#
Dell#configure
Dell(conf)#cam-acl-egress ?
default      Reset Egress CAM ACL entries to default setting
l2acl        Set L2-ACL entries
Dell(conf)#cam-acl-egress l2acl ?
<1-4>        Number of FP blocks for l2acl
Dell(conf)#cam-acl-egress l2acl 1 ?
ipv4acl       Set IPV4-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ?
ipv6acl       Set IPV6-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl ?
```

```
<0-4>          Number of FP blocks for IPV6 (multiples of 2)
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

deny (for IPv6 ACLs)

Configure a filter that drops IPv6 packets that match the filter criteria.

Syntax

```
deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count
[byte]] [dscp value] [order] [fragments] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.5(0.1)	Introduced on the Z9500.
Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny arp (for Extended MAC ACLs)

Configure an egress filter that drops ARP packets on egress ACL supported line cards. (For more information, refer to your line card documentation).

Syntax

```
deny arp {destination-mac-address mac-address-mask | any} vlan
vlan-id {ip-address | any | opcode code-number} [count [byte]]
[order] [log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation

	of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.
Command Modes	CONFIGURATION-EXTENDED-ACCESS-LIST
Command History	Version 9.5(0.1) Introduced on the Z9500. Version 9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms. Version 9.3(0.0) Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the flow-based <code>enable</code> command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny icmp (for Extended IPv6 ACLs)

Configure a filter to drop all or specific ICMP messages.

 **NOTE:** Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

Syntax

```
deny icmp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} [message-type]
[count [byte]] | [log [interval minutes] [threshold-in-msgs
[count]] [monitor]]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} command`

Parameters	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. You can enter a threshold in the range of 1-100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.
-----------------	--

Command Modes	ACCESS-LIST
--------------------------	-------------

Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
	Version 9.3.0.0	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny tcp (for IPv6 ACLs)

Configure a filter that drops TCP packets that match the filter criteria.

Syntax

```
deny tcp {source address mask | any | host ipv6-address}
[operator port [port]] {destination address | any | host ipv6-
address} [bit] [operator port [port]] [count [byte]] [log
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100..

	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults		By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.
Command Modes		ACCESS-LIST
Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
	Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information		When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny udp (for IPv6 ACLs)

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

Syntax	<pre>deny udp {source address mask any host ipv6-address} [operator port [port]] {destination address any host ipv6- address} [operator port [port]] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]</pre> To remove this filter, you have two choices: • Use the <code>no seq sequence-number</code> command syntax if you know the filter's sequence number • Use the <code>no deny udp {source address mask any host ipv6-address} {destination address any host ipv6-address} command</code>	
Parameters	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.	
Command Modes	ACCESS-LIST	
Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, Z9000, and MXL 10/40GbE Switch IO Module platforms.
	Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, Z9000, and MXL 10/40GbE Switch IO Module platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded	

expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs.

You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Z9500

Syntax	<code>ipv6 access-list access-list-name</code> To delete an access list, use the <code>no ipv6 access-list access-list-name</code> command.	
Parameters	<i>access-list-name</i>	Enter the access list name as a string, up to 140 characters.
Defaults	All access lists contain an implicit "deny any"; that is, if no match occurs, the packet is dropped.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series. Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation.

Related Commands

[show config](#) — views the current configuration.

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

Z9500

Syntax

`ipv6 control-plane egress-filter`

Defaults

Not enabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

permit (for IPv6 ACLs)

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax	<pre>permit {<i>ipv6-protocol-number</i> icmp ipv6 tcp udp} [count [byte]] [dscp <i>value</i>] [order] [fragments] [log [interval <i>minutes</i>] [threshold-in-msgs [<i>count</i>]]] [monitor]</pre> To remove this filter, you have two choices: • Use the <code>no seq sequence-number</code> command syntax if you know the filter's sequence number • Use the <code>no permit {<i>ipv6-protocol-number</i> icmp ipv6 tcp udp}</code> command	
Parameters	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.	
Command Modes	ACCESS-LIST	
Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
	Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.	

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit icmp (for IPv6 ACLs)

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

```
permit icmp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} [message-type]
[count [byte]] [log [interval minutes] [threshold-in-msgs
[count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL

in which you are creating the rule is applied to the monitored interface.

Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.	
Command Modes	ACCESS-LIST	
Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
	Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the <code>flow-based enable</code> command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).	
Related Commands	permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.	

permit tcp (for IPv6 ACLs)

Configure a filter to pass TCP packets that match the filter criteria.

Syntax

```
permit tcp {source address mask | any | host ipv6-address}  
[operator port [port]] {destination address | any | host ipv6-  
address} [bit] [operator port [port]] [count [byte]] [log  
[interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version 9.5(0.1)	Introduced on the Z9500.
Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that

new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

[permit \(for Standard IPv6 ACLs\)](#) – configures a filter to forward IPv6 packets.

permit udp (for IPv6 ACLs)

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax

```
permit udp {source address mask | any | host ipv6-address}  
[operator port [port]] {destination address | any | host ipv6-  
address} [operator port [port]] [count [byte]] [log [interval  
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.

	interval <i>minutes</i> (OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes. monitor (OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.
Command Modes	ACCESS-LIST
Command History	Version 9.5(0.1) Introduced on the Z9500. Version 9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms. Version 9.3.0.0 Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces. You can activate flow-based monitoring for a monitoring session by entering the <code>flow-based enable</code> command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).
Related Commands	permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.

seq (for IPv6 ACLs)

Assign a sequence number to a deny or permit the filter in an IPv6 access list while creating the filter.

Syntax	<pre>seq <i>sequence-number</i> {deny permit} {<i>ipv6-protocol-number</i> icmp ip tcp udp} {<i>source address mask</i> any host <i>ipv6-</i> <i>address</i>} {<i>destination address</i> any host <i>ipv6-address</i>} [<i>operator port [port]</i>] [<i>count [byte]</i>] [<i>log [interval minutes]</i>] [<i>threshold-in-msgs [count]</i>] [<i>monitor</i>]</pre> To delete a filter, use the <code>no seq <i>sequence-number</i></code> command.	
Parameters	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs <i>count</i>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminate with the <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
	monitor	(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
Defaults	By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.	
Command Modes	ACCESS-LIST	
Command History	Version 9.5(0.1)	Introduced on the Z9500.
	Version 9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
	Version 9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information	When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval. If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure	

ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

[permit \(for Standard IPv6 ACLs\)](#) – configures a filter to forward IPv6 packets.

test cam-usage

Verify that enough ACL CAM space is available for the IPv6 ACLs you have created.

Z9500

Syntax	<pre>test cam-usage service-policy input <i>policy-map-name</i> linecard {<i>slot-id</i> all}</pre>	
Parameters	input <i>policy-map name</i>	Enter the name of the policy-map to be verified.
	linecard <i>slot-id</i>	Enter the slot ID of the Z9500 line card, which contains the ports on which you assigned the ACL. Enter <code>all</code> to display IPv6 ACL information on all line cards. The range of Z9500 slot IDs is from 0 to 2.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.2.1.0	Introduced on the E-Series ExaScale.
	7.8.1.0	Introduced on the C-Series and E-Series TeraScale.
	8.4.2.1	Introduced on the S-Series.
	8.2.1.0	Introduced on the E-Series ExaScale.

Dell#test cam-usage service-policy input LauraMapTest linecard
2 port-set 1

Linecard	Portpipe	CAM Partition	Available CAM	Estimated CAM
per Port	Status			

--				
2	1	IPv4Flow	232	0
Allowed				
2	1	IPv6Flow	0	0
Allowed				

IPv6 Basics

IPv6 basic commands are supported on the Dell Networking operating system.

 **NOTE:** For information about the Dell Networking operating software version and platform that supports IPv6 in each software feature, refer to the *IPv6 Addressing* chapter of the *Dell Networking OS Configuration Guide*.

cam-ipv6 extended-prefix

Enable LPM CAM partitioning to support the storage of extended IPv6 (/65 to /128) route prefixes in LPM partition 1.

Z9500

Syntax

cam-ipv6 extended-prefix max-ipv6-prefixes

To remove LPM partitioning configuration, use no cam-ipv6 extended-prefix.

Parameters

max-ipv6-prefixes

Maximum number of extended IPv6 prefixes with the mask length of /65 to /128 that are supported in the LPM partition. The possible values are 1024, 2048, and 3072.

Defaults

LPM CAM is not partitioned with Partition 1. IPv6 /65 to /128 prefixes are not converted to /64 prefixes and saved in the LPM table. All the packets for extended IPv6 route prefixes are transmitted using the default route path.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information

You can partition the LPM table to store extended IPv6 route prefixes with /65 to /128 mask lengths. LPM CAM partitioning requires a switch reload to take effect.

To disable LPM CAM partitioning and return the number of the IPv6 /65-/128 route prefixes stored in Partition 1 to 0, enter the `no cam-ipv6 extended-prefix` command.

clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a Z9500 line card.

Z9500

Syntax	<code>clear ipv6 fib linecard slot-id</code>	
Parameters	linecard slot-id	Enter the slot ID of a Z9500 line card. Valid slot IDs are from 0 to 2.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

Z9500

Syntax	<code>clear ipv6 route {* ipv6-address prefix-length}</code>
---------------	--

Parameters

*	Enter the * to clear (refresh) all routes from the IPv6 routing table.
<i>ipv6-address prefix-length</i>	Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.
	NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

Z9500

Syntax

```
clear ipv6 mld_host
```

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

ipv6 address

Configure an IPv6 address to an interface.

Z9500

Syntax

```
ipv6 address {ipv6-address prefix-length}
```

To remove the IPv6 address, use the `no ipv6 address {ipv6-address prefix-length}` command.

Parameters

***ipv6-address
prefix-length***

Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Updated Usage Information.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support on the management Ethernet port.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the “no” form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

Example

```
Dell(conf)#interface tengigabitethernet 1/0
Dell(conf-if-te-1/0)#ipv6 address ?
X:X:X:X::X IPv6 address
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 /96
Dell(conf-if-te-1/0)#show config
!
interface TenGigabitEthernet 1/0
    no ip address
    ipv6 address 2002:1:2::3 /96
    no shutdown
Dell(conf-if-te-1/0)#
```

ipv6 address eui64

Configure IPv6 EUI64 address configuration on the interface.

Z9500

Syntax

```
ipv6 address {ipv6-address prefix-length} eui64
```

To disable IPv6 EUI64 address autoconfiguration, use the `no ipv6 address {ipv6-address prefix-length} eui64` command.

Parameters

***ipv6-address
prefix-length***

Enter the IPv6 prefix in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults	none						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2(0.0)	Introduced.
Version	Description						
9.2(1.0)	Introduced on the Z9500.						
9.2(0.0)	Introduced.						
Usage Information	This command allows you to create an EUI64 address based on the specified prefix and MAC address only. Prefixes may be configured on the interface using the <code>ipv6 nd prefix</code> command without creating an EUI64 address.						
Example	<pre>Dell(conf)#int ten 0/4 Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64 Dell(conf)#int ten 0/6 Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64</pre>						

ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets per second that can be sent per second.

Z9500

Syntax	<pre>ipv6 control-plane icmp error-rate-limit {1-200}</pre> To restore the default value, use the <code>no ipv6 control-plane icmp error-rate-limit</code> command.
Parameters	pps Enter the maximum number of error packets generated per second. The range is from 1 to 200, where 0 disables the rate-limiting.
Default	100 pps
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

Z9500

Syntax `ipv6 flowlabel-zero`
To disable the 0 from being set in the field and allow the rotocol operations to fill the field, use the `no ipv6 flowlabel-zero` command.

Default Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, set the new flowlabel to zero.

ipv6 host

Assign a name and IPv6 address the host-to-IPv6 address mapping table uses.

Z9500

Syntax	<code>ipv6 host name ipv6-address</code> To remove an IP host, use the <code>no ipv6 host name {ipv6-address}</code> .	
Parameters	name	Enter a text string to associate with one IP address.
	ipv6-address	Enter the IPv6 address (X:X:X:X::X) to be mapped to the name.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.1.0	Introduced on the E-Series TeraScale.

ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

Z9500

Syntax	<code>ipv6 name-server ipv6-address [ipv6-address2... ipv6-address6]</code> To remove a name server, use the <code>no ipv6 name-server ipv6-address</code> command.
--------	--

Parameters	<i>ipv6-address</i>	Enter the IPv6 address (X:X:X:X::X) of the name server to be used. Note: The :: notation specifies successive hexadecimal fields of zeros.														
	<i>ipv6-address2...</i> <i>ipv6-address6</i>	(OPTIONAL) Enter up to five more IPv6 addresses, in the x:x:x:x::x format, of name servers to be used. Separate the IPv6 addresses with a space.														
Defaults	none															
Command Modes	CONFIGURATION															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.4.2.1</td><td>Introduced on the C-Series and S-Series.</td></tr><tr><td>8.4.1.0</td><td>Introduced on the E-Series TeraScale.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.4.2.1	Introduced on the C-Series and S-Series.	8.4.1.0	Introduced on the E-Series TeraScale.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
9.0.0.0	Introduced on the Z9000.															
8.3.19.0	Introduced on the S4820T.															
8.3.7.0	Introduced on the S4810.															
8.4.2.1	Introduced on the C-Series and S-Series.															
8.4.1.0	Introduced on the E-Series TeraScale.															
Usage Information	You can separately configure both IPv4 and IPv6 domain name servers.															

ipv6 nd dad attempts

To perform duplicate address detection (DAD) on the management interface, configure the number of neighbor solicitation messages that are sent.

Z9500

Syntax	<code>ipv6 nd dad attempts {number of attempts}</code> To restore the default value, use the <code>no ipv6 nd dad attempts</code> command.	
Parameters	<i>number of attempts</i>	Enter the number of attempts to be made to detect a duplicate address. The range is from 0 to 15. Setting the value to 0 disables DAD on the interface.

Default	3 attempts										
Command Modes	INTERFACE (management interface only)										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										

ipv6 nd dns-server

Configures Recursive DNS Server (RDNSS) addresses to be distributed via IPv6 router advertisements to an IPv6 device.

Syntax	<pre>ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime infinite}</pre> To remove the IPv6 RDSS configuration, use <code>no ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime infinite}</code>	
Parameters	<i>ipv6-RDNSS-address</i>	Enter the IPv6 Recursive DNS Server's (RDNSS) address. You can specify up to 4 IPv6 RDNSS server addresses.
	<i>lifetime</i>	Enter the lifetime in seconds. The amount of time the IPv6 host can use the IPv6 RDNSS address for name resolution. The range is 0 to 4294967295 seconds. When you specify the maximum lifetime value of 4294967295 or <i>infinite</i> , the lifetime does not expire. A value of 0 indicates to the host that the RDNSS address should not be used. You must specify a lifetime using the <i>lifetime</i> or <i>infinite</i> parameter.
	<i>infinite</i>	Enter the keyword <i>infinite</i> to specify that the RDNSS lifetime does not expire.
Defaults	Not Configured	

Command Modes	INTERFACE CONFIG
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command. Version 9.5(0.0) Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	Use this command to add, edit, or delete an IPv6 RDNSS address and lifetime value. You can configure up to four IPv6 RDNSS addresses. You must specify a lifetime using the lifetime or infinite parameter.
Example	Dell(conf-if-te-0/1)#ipv6 nd dns-server 1000::1 1

ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

Z9500

Syntax	<code>ipv6 nd prefix {<i>ipv6-prefix</i> <i>prefix-length</i> default} [no-advertise] [no-autoconfig] [no-rtr-address] [off-link] [lifetime {<i>valid</i> infinite} {<i>preferred</i> infinite}]</code>	
Parameters		
	<i>ipv6-prefix</i>	Enter an IPv6 prefix.
	<i>prefix-length</i>	Enter the prefix then the prefix length. The length range is from 0 to 128.
	default	Enter the keyword <code>default</code> to set default parameters for all prefixes.
	no-advertise	Enter the keyword <code>no-advertise</code> to prevent the specified prefix from being advertised.
	no-autoconfig	Enter the keywords <code>no-autoconfig</code> to disable Stateless Address Autoconfiguration.
	no-rtr-address	Enter the keyword <code>no-rtr-address</code> to exclude the full router address from router advertisements (the R bit is not set).
	off-link	Enter the keywords <code>off-link</code> to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
	<i>valid-lifetime</i> infinite	Enter the amount of time that the prefix is advertised, or enter <code>infinite</code> for an unlimited amount of time. The range is from 0 to 4294967295. The default is 2592000 . The

		maximum value means that the preferred lifetime does not expire for the valid-life time parameter.												
	<i>preferred-lifetime</i> infinite	Enter the amount of time that the prefix is preferred, or enter <i>infinite</i> for an unlimited amount of time. The range is from 0 to 4294967295. The default is 604800 . The maximum value means that the preferred lifetime and does not expire.												
Command Modes	INTERFACE													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.2.0</td><td>Introduced on the E-Series TeraScale, C-Series, and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.2.0	Introduced on the E-Series TeraScale, C-Series, and S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
8.3.2.0	Introduced on the E-Series TeraScale, C-Series, and S-Series.													
Usage Information	By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the <i>default</i> keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the <i>ipv6 nd prefix default no-autoconfig</i> command.													

ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

Z9500

Syntax	<pre>ipv6 neighbor {ipv6-address} {interface interface} {hardware_address}</pre> To remove a static IPv6 entry from the IPv6 neighbor discovery, use the <i>no ipv6 neighbor {ipv6-address} {interface interface}</i> command.	
Parameters	<i>ipv6-address</i>	Enter the IPv6 address of the neighbor in the x:x:x::x format.



NOTE: The :: notation specifies successive hexadecimal fields of zero.

interface
interface

Enter the keyword `interface` then the interface type and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

hardware_addr
ess

Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

Defaults

none

Command
Modes

CONFIGURATION

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage
Information

Neighbor Discovery Protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. It defines mechanisms for solving problems, such as:

- Router discovery: Hosts can locate routers residing on a link.
- Prefix discovery: Hosts can discover address prefixes for the link.
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor Unreachability Detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate Address Detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

Use the `ipv6 neighbor` command to manually configure the IPv6 address of a neighbor to be discovered by the switch.

ipv6 route

Establish a static IPv6 route.

Z9500

Syntax

```
ipv6 route ipv6-address prefix-length {ipv6-address | interface  
| interface ipv6-address} [distance] [tag value] [permanent]
```

To remove the IPv6 route, use the `no ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]` command.

Parameters

ipv6-address
prefix-length

Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383.
- For the null interface, enter the keyword `null` then zero (0).
- For a port channel interface, enter the keyword `port-channel` then the port channel number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `VLAN` then the vlan number. The range is from 1 to 4094.

If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.

	<i>ipv6-address</i> (OPTIONAL) Enter the forwarding router IPv6 address in the x:x:x:x format.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.																		
	<i>distance</i> (OPTIONAL) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.																		
	<i>tag value</i> (OPTIONAL) Enter the keyword <code>tag</code> then a tag value number. The range is from 1 to 4294967295.																		
	<i>permanent</i> (OPTIONAL) Enter the keyword <code>permanent</code> to specify that the route is not to be removed, even if the interface assigned to that route goes down.  NOTE: If you disable the interface with an IPv6 address associated with the keyword <code>permanent</code>, the route disappears from the routing table.																		
Defaults	none																		
Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series TeraScale.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.2.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series TeraScale.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
9.0.0.0	Introduced on the Z9000.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.7.0	Introduced on the S4810.																		
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																		
8.2.1.0	Introduced on the E-Series ExaScale.																		
7.8.1.0	Introduced on the C-Series and S-Series.																		
7.4.1.0	Introduced on the E-Series TeraScale.																		
Usage Information	When the interface goes down, the system withdraws the route. The route is re-installed by the system when the interface comes back up. When a recursive resolution is "broken," the system withdraws the route. The route is re-installed the system when the recursive resolution is satisfied. After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.																		

Example

```
Dell(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>                               Distance metric for this route
permanent                             Permanent route
tag                                    Set tag for this route

Dell(conf)#ipv6 route 55::0 /64 ?
X:X:X:X::X                             Forwarding router's address
fortyGigE                             FortyGigabit Ethernet interface
loopback                              Loopback interface
null                                   Null interface
port-channel                          Port channel interface
tenGigabitethernet                   TenGigabit Ethernet interface
vlan                                  VLAN interface

Dell(conf)#ipv6 route 55::0 /64 tengigabitethernet 2/0 66::1 ?
<1-255>                               Distance metric for this route
permanent                             Permanent route
tag                                    Set tag for this route
Dell#
```

Related Commands

[show ipv6 route](#) — views the IPv6 configured routes.

ipv6 unicast-host-route

Enable the storage of extended IPv6 route prefixes (/65 to /128) in the L3 host table.

Z9500

Syntax

```
[no] ipv6 unicast-host-route
```

Defaults

Enabled; by default, extended IPv6 route prefixes are stored only in the L3 host table.

Command Modes

CONFIGURATION

Command History

Version

Description

9.5(0.1)

Introduced on the Z9500.

9.3(0.1)

Introduced on the S6000.

Usage Information

Use this command to enable programming of extended IPv6 (/65 to /128) route prefixes in the L3 host table. A warning message is displayed after you enter the command stating that this setting takes effect for existing routes only when IPv6 route prefixes are cleared from the LPM routing table (RTM). To enable storage of extended IPv6 route prefixes in the LPM table, disable this setting by entering the `no ipv6 unicast-host-route` command.

Example

```
Dell(conf)# ipv6 unicast-host-route
Warning: Command will take effect for existing routes only
when IPv6
route prefixes are cleared from RTM
Dell(conf)#no ipv6 unicast-host-route
```

```
Warning: Command will take effect for existing routes only
when IPv6
route prefixes are cleared from RTM
Dell(conf) #
```

ipv6 unicast-routing

Enable IPv6 Unicast routing.

Z9500

Syntax	<pre>ipv6 unicast-routing</pre> To disable unicast routing, use the <code>no ipv6 unicast-routing</code> command.																		
Defaults	Enabled																		
Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.4.2.1</td><td>Introduced on the S-Series.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series TeraScale.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.4.2.1	Introduced on the S-Series.	8.2.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the C-Series.	7.4.1.0	Introduced on the E-Series TeraScale.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
9.0.0.0	Introduced on the Z9000.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.7.0	Introduced on the S4810.																		
8.4.2.1	Introduced on the S-Series.																		
8.2.1.0	Introduced on the E-Series ExaScale.																		
7.8.1.0	Introduced on the C-Series.																		
7.4.1.0	Introduced on the E-Series TeraScale.																		
Usage Information	Because this command is enabled by default, it does not appear in the running configuration. When you disable unicast routing, the <code>no ipv6 unicast-routing</code> command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, the system generates a syslog message indicating the action. Disabling unicast routing on an E-Series chassis causes the following behavior: static and protocol learned routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated																		

- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered

show cam-ipv6 extended-prefix

Display the currently configured and next-boot settings for extended IPv6 prefixes (/65 to /128) in LPM CAM.

Z9500

Syntax `show cam-ipv6 extended-prefix`

Defaults None

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information You can use this command to view the maximum number of extended IPv6 prefix entries supported in LPM CAM. The output displays the current value and the new value applicable after a switch reload.

Example

```
Dell#show cam-ipv6 extended-prefix
Cam-Ipv6-LPM Extended Prefix
-----
Current Settings
cam-ipv6-max-/65-to-/128-Prefix : 2048
Dell(conf) #
```

show ipv6 cam linecard

Displays the IPv6 CAM entries for the specified line card and port pipe.

Z9500

Syntax `show ipv6 cam linecard slot-id port-set {0-3} [summary | ipv6-address]`

Parameters	line card slot-id	Enter the slot ID of the line card. The range of Z9500 slot IDs is from 0 to 2.
	port-set	Enter the keyword <code>port-set</code> followed by the port-pipe number. The range of Z9500 port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.
	summary	(OPTIONAL) Enter the keyword <code>summary</code> to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.
	ipv6-address	Enter the IPv6 address in the x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults	none
Command Modes	- EXEC - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.1	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.

Usage Information



NOTE: If a route has a mask greater than 64, no output is displayed but an equivalent /64 entry is listed in the `show ipv6 cam linecard {0-2} port-set {0-3}` output. Similarly, if there is more than one ECMP object with a destination route that has a mask greater than 64, if the first 64 bits in the destination routes of the ECMP objects are the same, only one route is installed in CAM even though multiple ECMP path entries exist.

Example

```
Dell# show ipv6 interface linecard 0
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
    Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64

Dell# show ipv6 interface linecard 0 configured
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
    Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64

Dell# show ipv6 cam linecard 0 port-set 2 summary

Total number of CAM entries   = 155648
```



```

Number of CAM entries used by NBR entries = 0
Number of CAM entries used by Prefix entries = 1
Section  Current Use Initial Size
-----
128      0          147519
127      0           63
126      0           63
125      0           63
124      0           63
123      0           63
122      0           63
121      0           63
120      0           63
119      0           63
118      0           63
117      0           63
116      0           63
115      0           63
--More--

```

show ipv6 control-plane icmp

Displays the status of the icmp control-plane setting for the error eate limit setting.

Z9500

Syntax `show ipv6 control-plane icmp`

Default 100

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands [ipv6 flowlabel-zero](#) — Configure IPv6 address auto-configuration for the management interface.

show ipv6 fib linecard

View all FIB entries.

Z9500

Syntax	show ipv6 fib linecard slot-id [summary ipv6-address]	
Parameters	linecard slot-id	Enter the slot ID of the line card. The range of Z9500 slot IDs is from 0 to 2.
	summary	(OPTIONAL) Enter the keyword summary to view a summary of entries in IPv6 cam.
	ipv6-address	Enter the IPv6 address in the x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.
 NOTE: The :: notation specifies successive hexadecimal fields of zeros.		

Command Modes	- EXEC - EXEC Privilege
---------------	---

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.
-----------------	---

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.

Usage Information	Host tables are not stored in CAM tables on S-Series platforms. Entries for camIndex displays as zero (0) on the show ipv6 fib linecard output for neighbor entries, such as address resolution protocol (ARP) entries.
-------------------	---

Example	<pre>Dell# show ipv6 fib linecard 0 summary Total Number of Routes in the FIB database is 0 Total Number of Routes in the CAM is 1 Total Number of Routes which can be entered in CAM is 155647 IPC Messages Received from RTM 158 [Add route requests 0; Delete Route requests 0] [Clear Route requests 0] IPC Messages Received from NDPM 0 Section Current Use</pre>
---------	---

```

-----
128      0
127      0
126      0
125      0
124      0
123      0
122      0
121      0
120      0
119      0
118      0
117      0
116      0
--More--

```

show ipv6 flowlabel-zero

Display the flow label zero setting.

Z9500

Syntax `show ipv6 flowlabel-zero`

Default Disabled

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands [ipv6 nd dad attempts](#) — Configure system to set the flow label field in the packets to zero.

show ipv6 interface

Display the status of interfaces configured for IPv6.

Z9500

Syntax	<pre>show ipv6 interface interface [linecard slot-id] [brief] [configured][loopback interface-number] [managementethernet slot/port] [port-channel number][tengigabitethernet slot slot/port] [fortyGigE slot slot/port] [tunnel tunnel-id] [vlan vlan-id]</pre>	
Parameters	interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword <code>Loopback</code> then a number from 0 to 16383. • For the Null interface, enter the keyword <code>null</code> then zero (0). • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a tunnel interface, enter the keyword <code>tunnel</code> then the tunnel ID. • For a VLAN interface, enter the keyword <code>VLAN</code>. • For a port channel interface, enter the keywords <code>port-channel</code>.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify the Z9500 ports on a line card. The range of slot IDs is from 0 to 2.
	brief	(OPTIONAL) View a summary of IPv6 interfaces.
	configured	(OPTIONAL) View information on all IPv6 configured interfaces.
	managementethernet slot/port	(OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).
	loopback	(OPTIONAL) View information for IPv6 Loopback interfaces.
	port-channel	(OPTIONAL) View information for IPv6 port channels.
	tengigabitethernet	(OPTIONAL) View information for an IPv6 tengigabitethernet interface.
	fortyGigE	(OPTIONAL) View information for an IPv6 fortygigabitethernet interface.
	tunnel tunnel-id	(OPTIONAL) View information for a tunnel interface.

	vlan	(OPTIONAL) View information for IPv6 VLANs.																								
Defaults	none																									
Command Modes	- EXEC - EXEC Privilege																									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Added support for IPv6 recursive DNS addresses.</td></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2.(0.0)</td><td>Added support for tunnel interface.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr><tr><td>8.4.2.1</td><td>Introduced on the S-Series.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale. Added support for the <code>managementethernet slot/port</code> parameter.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series TeraScale.</td></tr></table>		Version	Description	9.5(0.1)	Added support for IPv6 recursive DNS addresses.	9.2(1.0)	Introduced on the Z9500.	9.2.(0.0)	Added support for tunnel interface.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.4.2.1	Introduced on the S-Series.	8.2.1.0	Introduced on the E-Series ExaScale. Added support for the <code>managementethernet slot/port</code> parameter.	7.8.1.0	Introduced on the C-Series.	7.4.1.0	Introduced on the E-Series TeraScale.
Version	Description																									
9.5(0.1)	Added support for IPv6 recursive DNS addresses.																									
9.2(1.0)	Introduced on the Z9500.																									
9.2.(0.0)	Added support for tunnel interface.																									
9.0.0.0	Introduced on the Z9000.																									
8.3.19.0	Introduced on the S4820T.																									
8.3.7.0	Introduced on the S4810.																									
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																									
8.4.2.1	Introduced on the S-Series.																									
8.2.1.0	Introduced on the E-Series ExaScale. Added support for the <code>managementethernet slot/port</code> parameter.																									
7.8.1.0	Introduced on the C-Series.																									
7.4.1.0	Introduced on the E-Series TeraScale.																									
Usage Information	The Management port is enabled by default (<code>no shutdown</code>). If necessary, use the <code>ipv6 address</code> command to assign an IPv6 address to the Management port.																									
Example	<pre>Dell# show ipv6 interface linecard 0 TenGigabitEthernet 0/2 is down, line protocol is down IPV6 is enabled Link Local address: fe80::7686:7aff:feff:6f08 Global Unicast address(es): 10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL) Remaining lifetime: infinite Global Anycast address(es): Joined Group address(es): ff02::1 ff02::2 ff02::1:ff00:8 ff02::1:ffff:6f08 ND MTU is 0 ICMP redirects are not sent DAD is enabled, number of DAD attempts: 3 ND reachable time is 27000 milliseconds ND base reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND advertised retransmit interval is 0 milliseconds</pre>																									

```

ND router advertisements are sent every 200 to 600 seconds
ND router advertisements live for 1800 seconds
ND advertised hop limit is 64
IPv6 hop limit for originated packets is 64

Dell# show ipv6 interface linecard 0 configured
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
    Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64

Dell# show ipv6 interface linecard 0 configured
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
    Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64

Dell# show ipv6 interface linecard 1 configured | grep ff02
  ff02::1
  ff02::2
  ff02::1:ff00:6
  ff02::1:ffff:6f08
  ff02::1
  ff02::2

```

```
ff02::1:ff00:4
ff02::1:ffff:6f08
```

show ipv6 mld_host

Display the IPv6 MLD host counters.

Z9500

Syntax `show ipv6 mld_host`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information The following describes the `show ipv6 mld-host` command shown in the following example.

Field	Description
Valid MLD Packets	The total number of packets received and sent from the last time the elapsed time was cleared.
Reports	The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.
Leaves	The number of Multicast leaves that have been sent.
MLDv1 queries	The number of MLDv1 queries that have been received.
MLDv2 queries	The number of MLDv2 queries that have been received.
Malformed Packets	The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

Example

```
MLD Host Traffic Counters
Elapsed time since counters cleared: 0028:33:52
      Received      Sent
Valid MLD Packets  97962    18036
Reports           79962    18034
```

```

Leaves          ----      0
MLDv2 Queries   18000     ----
MLDv1 Queries    0        ----
Errors:
Malformed Packets: 4510

```

show ipv6 neighbors

Display information about the IPv6 neighbors learned on Z9500 CPUs.

Z9500

Syntax	<code>show ipv6 neighbors [cpu rp] [ipv6-address] {ipv6-address} [interface interface]</code>	
Parameters	cpu rp	Enter the keywords <code>cpu rp</code> to display information about IPv6 neighbors learned only on the Route Processor.
	<i>ipv6-address</i>	Enter the IPv6 address of a neighbor to display information about the specified device.
	<i>interface</i>	Enter one of the following keywords with slot/port or number to display information about the IPv6 neighbors learned on the specified port, port channel, or VLAN: • For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port-channel interface, enter the keyword <code>port-channel</code> with a port-channel number. The range of port-channel numbers is from 1 to 128. • For VLAN interfaces, enter the keyword <code>vlan</code> with a VLAN ID from 1 to 4094.
Defaults	Display information about IPv6 neighbors learned on all Z9500 CPUs, including the Route Processor and line-card processors.	
Command Modes	• EXEC • EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Added support for BFD for BGP on the S4810.
8.4.1.3	Added support for BFD for BGP on the E-Series ExaScale.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Added support for BFD for VLAN and port-channel interfaces on the E-Series.
7.4.1.0	Introduced BFD on physical ports on the E-Series.

Example

```
Dell#show ipv6 neighbors

*      - Active session role
Ad Dn - Admin Down
B      - BGP
C      - CLI
I      - ISIS
O      - OSPF
R      - Static Route (RTM)

    LocalAddr  RemoteAddr  Interface  State  Rx-int  Tx-int  Mult
Clients
* 10.1.3.2    10.1.3.1    Te 1/3     Up     300    250    3    C
```

Example (Detail)

```
Dell#show ipv6 neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: TenGigabitEthernet 1/3
State: Up
Configured parameters:
  TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
  TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
  TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
  Number of packets received from neighbor: 376
  Number of packets sent to neighbor: 314
  Number of state changes: 2
  Number of messages from IFA about port state change: 0
```

show ipv6 route

Displays the IPv6 routes.

Z9500

Syntax

```
show ipv6 route [ipv6-address prefix-length] [hostname] [all]
[bgp as number] [connected] [isis tag] [list prefix-list name]
[ospf process-id] [rip] [static] [summary]
```

Parameters

***ipv6-address
prefix-length***

(OPTIONAL) Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

hostname

(OPTIONAL) View information for this IPv6 routes with Host Name.

all

(OPTIONAL) View information for all IPv6 routes.

bgp

(OPTIONAL) View information for all IPv6 BGP routes.

connected

(OPTIONAL) View only the directly connected IPv6 routes.

isis

(OPTIONAL) View information for all IPv6 IS-IS routes.

list

(OPTIONAL) View the IPv6 prefix list.

ospf

(OPTIONAL) View information for all IPv6 OSPF routes.

rip

(OPTIONAL for E-Series only) View information for all IPv6 RIP routes.

static

(OPTIONAL) View only routes configured by the `ipv6 route` command.

summary

(OPTIONAL) View a brief list of the configured IPv6 routes.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

The following describes the `show ipv6 route` command shown in the following examples.

Field	Description
(undefined)	Identifies the type of route: • L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter-area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.

Field	Description
Last Change	Identifies when the route was last changed or configured.

Example

```
Dell#show ipv6 route

Codes:C-connected, L-local, S-static, R-RIP,
      B-BGP, IN-internal BGP, EX-external BGP,LO-Locally Originated,
      O-OSPF, IA-OSPF inter area, N1-OSPF NSSA external type 1,
      N2-OSPF NSSA external type 2, E1-OSPF external type 1,
      E2-OSPF external type 2, i-IS-IS, L1-IS-IS level-1,
      L2-IS-IS level-2, IA- IS-IS inter area, *-candidate default,
Gateway of last resort is not set

      Destination Dist/Metric, Gateway, Last Change
-----
C 2001::/64 [0/0]
   Direct, Te 1/1, 00:28:49
C 2002::/120 [0/0]
   Direct, Te 1/1, 00:28:49
C 2003::/120 [0/0]
   Direct, Te 1/1, 00:28:49
C 2004::/32 [0/0]
   Direct, Te 1/1, 00:28:49
L fe80::/10 [0/0]
   Direct, Nu 0, 00:29:09
```

Example (Summary)

```
Dell#show ipv6 route summary

Route Source  Active Routes  Non-active Routes
connected     5                0
static        0                0
Total         5                0
Total 5 active route(s) using 952 bytes
```

Intermediate System to Intermediate System (IS-IS)

The intermediate system to intermediate system (IS-IS) is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the *Dell Networking OS Configuration Guide*.



NOTE: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Z9500

Syntax	adjacency-check To disable adjacency check, use the <code>no adjacency-check</code> command.				
Defaults	Enabled.				
Command Modes	- ROUTER ISIS (<i>for IPv4</i>) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.
Version	Description				
9.5(0.1)	Introduced on the Z9500.				

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced on the E-Series.

Usage Information To perform protocol-support consistency checks on hello packets, use this command. The adjacency-check is enabled by default.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

Z9500

Syntax `advertise {level1-into-level2 | level2-into-level1} prefix-list-name`

To return to the default, use the `no advertise {level1-into-level2 | level2-into-level1} [prefix-list-name]` command.

Parameters

level1-into-level2	Enter the keywords <code>level1-into-level2</code> to advertise Level 1 routes into Level 2 LSPs. This setting is the default.
level2-into-level1	Enter the keywords <code>level2-into-level1</code> to advertise Level 2 inter-area routes into Level 1 LSPs. This behavior is described in RFC 2966.
<i>prefix-list-name</i>	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults **level1-into-level2** (Level 1 to Level 2 leaking enabled.)

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.

	Version	Description
	9.0.2.0	Introduced on the S6000.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.3.11.1	Introduced on the Z9000.
	7.5.1.0	Added IPv6 ISIS support.
	6.3.1.0	Version 6.3.1.0 Introduced
Usage Information	You cannot disable leaking from one level to another; however, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all routes are leaked. You can find more information in IETF RFC 2966, <i>Domain-wide Prefix Distribution with Two-Level IS-IS</i>.	

area-password

Configure a hash message authentication code (HMAC) password for an area.

Z9500

Syntax	<pre>area-password [hmac-md5 <i>encryption-type</i>] <i>password</i></pre> To delete a password, use the <code>no area-password</code> command.	
Parameters	hmac-md5 (OPTIONAL) Enter the keywords <code>hmac-md5</code> to encrypt the password. <i>encryption-type</i> (OPTIONAL) Enter 7 to encrypt the password using DES. <i>password</i> Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.	
Defaults	Not configured.	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

To prevent the link state database from receiving incorrect routing information from unauthorized routers, use the `area-password` command on routers within an area.

The configured password injects into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

- [domain-password](#) — allows you to set the authentication password for a routing domain.
- [isis password](#) — allows you to configure an authentication password for an interface.

clear config

Clear IS-IS configurations that display under the *router isis* heading of the `show running-config` command output.

Z9500

Syntax `clear config`

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.



CAUTION: Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

clear isis

Restart the IS-IS process. All IS-IS data is cleared.

Z9500

Syntax	<code>clear isis [tag] {* database traffic}</code>		
Parameters	tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.	
	*	Enter the keyword * to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.	
	database	Clears IS-IS LSP database information.	
	traffic	Clears IS-IS counters.	
Command Modes	EXEC Privilege		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .		

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

clns host

Define a name-to-network service mapping point (NSAP) that you use with commands that require NSAPs and system IDs.

Z9500

Syntax	<code>clns host name nsap</code>													
Parameters	name	Enter an alphanumeric string to identify the name-to-NSAP mapping.												
	nsap	Enter a specific NSAP address that is associated with the name parameter.												
Defaults	Not configured.													
Command Modes	ROUTER ISIS													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.0.2.0	Introduced on the S6000.													
8.3.19.0	Introduced on the S4820T.													
8.3.12.0	Introduced on the S4810.													
8.3.11.1	Introduced on the Z9000.													
Usage Information	To configure a shortcut name that you can use instead of entering a long string of numbers associated with an NSAP address, use this command.													
Related Commands	hostname dynamic — enables dynamic learning of host names from routers in the domain and allows the routers to advertise the host names in LSPs.													

debug isis

Enable debugging for all IS-IS operations.

Z9500

Syntax	<code>debug isis</code> To disable debugging of IS-IS, use the <code>no debug isis</code> command.
--------	---

Command Modes	EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	Entering <code>debug isis</code> enables all debugging parameters. To display all debugging information in one output, use this command. To turn off debugging, you normally enter separate <code>no</code> forms of each command. To disable all debug messages for IS-IS at once, enter the <code>no debug isis</code> command.												

debug isis adj-packets

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

Z9500

Syntax	<pre>debug isis adj-packets [interface]</pre> To turn off debugging, use the <code>no debug isis adj-packets [interface]</code> command.	
Parameters	<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Command Modes	EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.2)</td><td>Introduced on the Z9000.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Introduced on the Z9000.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.2(0.2)	Introduced on the Z9000.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												

debug isis local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

Z9500

Syntax	<pre>debug isis local-updates [<i>interface</i>]</pre> To turn off debugging, use the <code>no debug isis local-updates [<i>interface</i>]</code> command.
Parameters	<i>interface</i> (OPTIONAL) Identifies the interface type slot/port as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

debug isis snp-packets

To debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets, enable debugging on a specific interface and provides diagnostic information.

Z9500

Syntax

```
debug isis snp-packets [interface]
```

To turn off debugging, use the `no debug isis snp-packets [interface]` command.

Parameters

interface

(OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

debug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Z9500

Syntax `debug isis spf-triggers`
To turn off debugging, use the `no debug isis spf-triggers` command.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced.

debug isis update-packets

Enable debugging on link state PDUs (LSPs) that a router detects.

Z9500

Syntax `debug isis update-packets [interface]`
To turn off debugging, use the `no debug isis update-packets [interface]` command.

Parameters

<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following:
	• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

default-information originate

Generates a default route into an IS-IS routing domain and controls the distribution of default information.

Z9500

Syntax `default-information originate [always] [metric metric] [route-map map-name]`
To disable the generation of a default route into the specified IS-IS routing domain, use the `no default-information originate [always] [metric metric] [route-map map-name]` command.

Parameters

always	(OPTIONAL) Enter the keyword <code>always</code> to have the default route always advertised.
metric <i>metric</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to assign to the route. The range is from 0 to 16777215.
route-map <i>map-name</i>	(OPTIONAL) A default route the routing process generates if the route map is satisfied.

Defaults Not configured.

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Usage Information When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route advertises depends on the `metric-style` command configuration. If the `metric-style` command is set for Narrow mode and the metric value in the `default-information originate` command is set to a number higher than 63, the metric value advertised in the LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `default-information originate` command is advertised.

Related Commands

- [redistribute](#) — redistributes routes from one routing domain to another routing domain.
- [isis metric](#) — configures a metric for an interface.
- [metric-style](#) — sets the metric style for the router.
- [show isis database](#) — displays the IS-IS link state database.

description

Enter a description of the IS-IS routing protocol.

Z9500

Syntax

```
description {description}
```

To remove the description, use the `no description {description}` command.

Parameters

description

Enter a description to identify the IS-IS protocol (80 characters maximum).

Defaults

none

Command Modes

ROUTER ISIS

Command History

Version

Description

9.5(0.1)

Introduced on the Z9500.

9.0.2.0

Introduced on the S6000.

8.3.19.0

Introduced on the S4820T.

8.3.12.0

Introduced on the S4810.

8.3.11.1

Introduced on the Z9000.

pre-7.7.1.0

Introduced.

Related Commands

[router isis](#) — Enter ROUTER mode on the switch.

distance

Define the administrative distance for learned routes.

Z9500

Syntax

distance weight [ip-address mask [prefix-list]]

To return to the default values, use the no distance weight command.

Parameters

weight

The administrative distance value indicates the reliability of a routing information source. The range is from 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.) The default is **115**.

ip-address mask

(OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.

prefix-list

(OPTIONAL) Enter the name of a prefix list name.

Defaults

weight = **115**

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced.

Usage Information

The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

Filter network prefixes received in updates.

Z9500

Syntax `distribute-list prefix-list-name in [interface]`
To return to the default values, use the `no distribute-list prefix-list-name in [interface]` command.

Parameters	<i>prefix-list-name</i>	Specify the prefix list to filter prefixes in routing updates.
	<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a SONET interface, enter the keyword <code>sonet</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Related Commands

- [distribute-list out](#) — suppresses networks from being advertised in updates.
- [redistribute](#) — redistributes routes from one routing domain to another routing domain.

distribute-list out

Suppress network prefixes from being advertised in outbound updates.

Z9500

Syntax

```
distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]
```

To return to the default values, use the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

Parameters

<i>prefix-list-name</i>	Specify the prefix list to filter prefixes in routing updates.
<i>connected</i>	(OPTIONAL) Enter the keyword <code>connected</code> for directly connected routing process.
<i>ospf process-id</i>	(OPTIONAL) Enter the keyword <code>ospf</code> then the OSPF process-ID number. The range is from 1 to 65535.
<i>bgp as number</i>	(OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.
<i>rip</i>	(OPTIONAL) Enter the keyword <code>rip</code> for RIP routes.
<i>static</i>	(OPTIONAL) Enter the keyword <code>static</code> for user-configured routing process.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.

	Version	Description
	9.0.2.0	Introduced on the S6000.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	7.5.1.0	Added IPv6 ISIS support.
	6.3.1.0	Introduced.
Usage Information	You can assign a name to a routing process so a prefix list IS applied to only the routes derived from the specified routing process.	
Related Commands	• distribute-list in — filters the networks received in updates. • redistribute — redistributes routes from one routing domain to another routing domain.	

distribute-list redistributed-override

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

Z9500

Syntax	<pre>distribute-list redistributed-override in</pre> To return to the default, use the <code>no distribute-list redistributed-override in</code> command.
Defaults	none
Command Modes	• ROUTER ISIS (<i>for IPv4</i>) • CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	7.8.1.0	Added IPv6 ISIS support.
	6.3.1.0	Introduced.
Usage Information	When you execute this command, IS-IS does not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.	

domain-password

Set the authentication password for a routing domain.

Z9500

Syntax	<code>domain-password [hmac-md5 <i>encryption-type</i>] <i>password</i></code> To disable the password, use the <code>no domain-password</code> command.	
Parameters	hmac-md5 (OPTIONAL) Enter the keywords <code>hmac-md5</code> to encrypt the password using MD5. <i>encryption-type</i> (OPTIONAL) Enter 7 to encrypt the password using DES. <i>password</i> Enter an alphanumeric string up to 16 characters long. If you do not specify an <code>encryption type</code> or <code>hmac-md5</code> keywords, the password is processed as plain text which provides limited security.	
Defaults	No default password.	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>6.3.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	8.3.11.1	Introduced on the Z9000.	6.3.1.0	Introduced.
Version	Description						
8.3.11.1	Introduced on the Z9000.						
6.3.1.0	Introduced.						
Usage Information	The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).						
Related Commands	• area-password — configures an IS-IS area authentication password. • isis priority — configures the authentication password for an interface.						

graceful-restart ietf

Enable graceful restart on an IS-IS router.

Z9500

Syntax	<pre>graceful-restart ietf</pre> To return to the default, use the <code>no graceful-restart ietf</code> command.														
Parameters	<table> <tr> <td>ietf</td><td>Enter <code>ietf</code> to enable graceful restart on the IS-IS router.</td></tr> </table>	ietf	Enter <code>ietf</code> to enable graceful restart on the IS-IS router.												
ietf	Enter <code>ietf</code> to enable graceful restart on the IS-IS router.														
Defaults	Graceful restart disabled.														
Command Modes	ROUTER ISIS														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>6.3.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	6.3.1.0	Introduced on the E-Series.
Version	Description														
9.5(0.1)	Introduced on the Z9500.														
9.0.2.0	Introduced on the S6000.														
8.3.19.0	Introduced on the S4820T.														
8.3.12.0	Introduced on the S4810.														
8.3.11.1	Introduced on the Z9000.														
6.3.1.0	Introduced on the E-Series.														
Usage Information	Every graceful restart enabled router's HELLO PDUs includes a restart TLV. This restart enables (re)starting as well as the existing ISIS peers to detect the GR														

capability of the routers on the connected network. A flag in the Restart TLV contains restart request (RR), restart acknowledge (RA) and suppress adjacency advertisement (SA) bit flags.

The ISIS graceful restart-enabled router can co-exist in mixed topologies where some routers are graceful restart-enabled and others are not. For neighbors that are not graceful restart-enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval

Set the graceful restart grace period, the time during that all graceful restart attempts are prevented.

Z9500

Syntax	<code>graceful-restart interval minutes</code> To return to the default, use the <code>no graceful-restart interval</code> command.	
Parameters	<i>minutes</i>	Enter the graceful-restart interval minutes. The range is from 1 to 20 minutes. The default is 5 minutes .
Defaults	5 minutes	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

Z9500

Syntax



NOTE: Set the t3 timer to adjacency on the restarting router when implementing this command.

`graceful-restart restart-wait seconds`

To return to the default, use the `no graceful-restart restart-wait` command.

Parameters

seconds Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is **30 seconds**.

Defaults

30 seconds

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

Related Commands

[graceful-restart t3](#) — configures the overall wait time before graceful restart completes.

graceful-restart t1

Set the graceful restart wait time before unacknowledged restart requests are generated. This wait time is the interval before the system sends a restart request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

Z9500

Syntax	<code>graceful-restart t1 {interval seconds retry-times value}</code>	
	To return to the default, use the <code>no graceful-restart t1</code> command.	
Parameters	interval	Enter the keyword <code>interval</code> to set the wait time. The range is from 5 to 120 seconds. The default is 5 seconds .
	retry-times	Enter the keywords <code>retry-times</code> to set the number of times the request interval is extended until a CSNP is received from the helping router. The range is from 1 to 10 attempts. The default is 1 .
Defaults	Refer to Parameters.	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart t2

Configure the wait time for the graceful restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

Z9500

Syntax	<code>graceful-restart t2 {level-1 level-2} seconds</code> To return to the default, use the <code>no graceful-restart t2</code> command.	
Parameters	level-1, level-2	Enter the keywords <code>level-1</code> or <code>level-2</code> to identify the database instance type to which the wait interval applies.
	seconds	Enter the <code>graceful-restart t2</code> time in seconds. The range is from 5 to 120 seconds. The default is 30 seconds .
Defaults	30 seconds	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart t3

Configure the overall wait time before graceful restart completes.

Z9500

Syntax	<code>graceful-restart t3 {adjacency manual} seconds</code> To return to the default, use the <code>no graceful-restart t3</code> command.
--------	---

Parameters	adjacency	Enter the keyword <code>adjacency</code> so that the restarting router receives the remaining time value from its peer and adjusts its T3 value so if you have configured this option.														
	manual	Enter the keyword <code>manual</code> to specify a time value that the restarting router uses. The range is from 50 to 120 seconds. The default is 30 seconds .														
Defaults	manual, 30 seconds															
Command Modes	ROUTER ISIS															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.3.1.0	Introduced on the E-Series.
Version	Description															
9.5(0.1)	Introduced on the Z9500.															
9.0.2.0	Introduced on the S6000.															
8.3.19.0	Introduced on the S4820T.															
8.3.12.0	Introduced on the S4810.															
8.3.11.1	Introduced on the Z9000.															
8.3.1.0	Introduced on the E-Series.															
Usage Information	The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command. Override the default restart-wait time by entering the <code>no graceful-restart restart-wait</code> command. When you disable <code>restart-wait</code>, the current adjacency hold time is used. Set the <code>t3</code> timer to <code>adjacency</code> on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value so only when you have configured <code>graceful-restart t3 adjacency</code>.															
Related Commands	graceful-restart restart-wait — enables the graceful restart maximum wait time before a restarting peer comes up.															

hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Z9500

Syntax `hello padding [multi-point | point-to-point]`
To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

Parameters

multi-point	(OPTIONAL) Enter the keywords <code>multi-point</code> to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keywords <code>point-to-point</code> to pad only point-to-point PDUs.

Defaults Both LAN and point-to-point hello PDUs are padded.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands [isis hello padding](#) — turns ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Z9500

Syntax	<code>hostname dynamic</code> To disable this command, use the <code>no hostname dynamic</code> command.												
Defaults	Enabled.												
Command Modes	ROUTER ISIS												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></tbody></table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	To build name-to-systemID mapping tables through the protocol, use this command. All <code>show</code> commands that display systems also display the hostname.												
Related Commands	clns host — defines a name-to-NSAP mapping.												

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

Z9500

Syntax	<code>ignore-lsp-errors</code> To return to the default values, use the <code>no ignore-lsp-errors</code> command.
Defaults	In IS-IS, the default deletes LSPs with internal checksum errors (<code>no ignore-lsp-errors</code>).

Command Modes	ROUTER ISIS												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	IS-IS normally purges LSPs with an incorrect data link checksum causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This process could cause disruption to your system operation.												

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

Z9500

Syntax	<pre>ip router isis [tag]</pre> To disable IS-IS on an interface, use the <code>no ip router isis [tag]</code> command.
Parameters	tag (OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.
Defaults	No processes are configured.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.0.2.0	Introduced on the S6000.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.3.11.1	Introduced on the Z9000.
	7.5.1.0	Introduced.
Usage Information	To assign a network entity title to enable IS-IS, use the <code>net</code> command.	
Related Commands	• net — configures an IS-IS network entity title (NET) for the routing process. • router isis — enables the IS-IS routing protocol.	

ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

Z9500

Syntax	<pre>ipv6 router isis [tag]</pre> To disable IS-IS routing, use the <code>no router isis [tag]</code> command.	
Parameters	tag	(OPTIONAL) This parameter is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.
Defaults	Not configured.	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.5.1.0	Introduced on the E-Series.
Version	Description										
8.3.19.0	Introduced on the S4820T.										
8.3.12.0	Introduced on the S4810.										
8.3.11.1	Introduced on the Z9000.										
7.5.1.0	Introduced on the E-Series.										
Usage Information	Configure a network entity title (the <code>net</code> command) to specify the area address and the router system ID. To establish adjacencies and establish dynamic routing, enable routing on one or more interfaces. You can configure only one IS-IS routing process to perform Level 2 routing. A <code>level-1-2</code> designation performs Level 1 and Level 2 routing at the same time.										
Related Commands	• net — configures an IS-IS network entity title (NET) for the routing process. • is-type — assigns a type for a given area.										

isis circuit-type

Configure the adjacency type on interfaces.

Z9500

Syntax	<pre>isis circuit-type {level-1 level-1-2 level-2-only}</pre> To return to the default values, use the <code>no isis circuit-type</code> command.	
Parameters	level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
	level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, a Level 2 adjacency is established. This setting is the default.
	level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.
Defaults	level-1-2	

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system must be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Z9500

Syntax `isis csnp-interval seconds [level-1 | level-2]`
To return to the default values, use the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is from 0 to 65535. The default is 10 .
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults seconds = **10**; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

You can configure Level 1 and Level 2 CSNP intervals independently.

isis hello-interval

Specify the length of time between hello packets sent.

Z9500

Syntax `isis hello-interval seconds [level-1 | level-2]`
To return to the default values, use the `no isis hello-interval [seconds] [level-1 | level-2]` command.

Parameters

seconds	Allows you to set the length of time between hello packet transmissions. The range is from 1 to 65535. The default is 10 .
level-1	(OPTIONAL) Select this value to configure the hello interval for Level 1. This value is the default.
level-2	(OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults seconds = **10**; **level-1** (if not otherwise specified)

Command Modes	INTERFACE												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	Hello packets are held for a length of three times the value of the hello interval. To conserve bandwidth and CPU usage, use a high hello interval seconds. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).												
Related Commands	isis hello-multiplier — specifies the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency as down.												

isis hello-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

Z9500

Syntax	<pre>isis hello-multiplier <i>multiplier</i> [level-1 level-2]</pre> To return to the default values, use the <code>no isis hello-multiplier [<i>multiplier</i>] [level-1 level-2]</code> command.	
Parameters	<i>multiplier</i>	Specifies an integer that sets the multiplier for the hello holding time. Never configure a hello-multiplier lower than the default (3). The range is from 3 to 1000. The default is 3 .
	level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
	level-2	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults	multiplier = 3 ; level-1 (if not otherwise specified)												
Command Modes	INTERFACE												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.												
Related Commands	isis hello-interval — specifies the length of time between hello packets.												

isis hello padding

Turn ON or OFF padding of hello PDUs from INTERFACE mode.

Z9500

Syntax	<pre>isis hello padding</pre> To return to the default, use the <code>no isis hello padding</code> command.				
Defaults	Padding of hello PDUs is enabled (ON).				
Command Modes	INTERFACE				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.
Version	Description				
9.5(0.1)	Introduced on the Z9500.				

	Version	Description
	9.0.2.0	Introduced on the S6000.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.3.11.1	Introduced on the Z9000.
Usage Information	Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF disables padding for the corresponding interface.	
Related Commands	hello padding — turns ON or OFF padding for LAN and point-to-point hello PDUs.	

isis ipv6 metric

Assign metric to an interface for use with IPv6 information.

Z9500

Syntax	<pre>isis ipv6 metric <i>default-metric</i> [level-1 level-2]</pre> To return to the default values, use the <code>no ipv6 isis metric [<i>default-metric</i>] [level-1 level-2]</code> command.	
Parameters	<i>default-metric</i> Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215. The default is 10. <i>level-1</i> (OPTIONAL) Enter the keywords <code>level-1</code> to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This value is the default. <i>level-2</i> (OPTIONAL) Enter the keywords <code>level-2</code> to configure the SPF calculation for Level 2 (inter-area) routing.	
Defaults	default-metric = 10 ; level-1 (if not otherwise specified)	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced on the E-Series.

Usage Information

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis metric

Assign a metric to an interface.

Z9500

Syntax

```
isis metric default-metric [level-1 | level-2]
```

To return to the default values, use the `no isis metric [default-metric] [level-1 | level-2]` command.

Parameters

<i>default-metric</i>	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 63 for narrow and transition metric styles and from 0 to 16777215 for wide metric styles. The default is 10 .
<i>level-1</i>	(OPTIONAL) Enter the keywords <code>level-1</code> to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This setting is the default.
<i>level-2</i>	(OPTIONAL) Enter the keywords <code>level-2</code> to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults

`default-metric` = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

Z9500

Syntax `isis network point-to-point`
To disable the feature, use the `no isis network point-to-point` command.

Defaults Not enabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

isis password

Configure an authentication password for an interface.

Z9500

Syntax `isis password [hmac-md5] password [level-1 | level-2]`
To delete a password, use the `no isis password [password] [level-1 | level-2]` command.

Parameters	encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
	hmac-md5	(OPTIONAL) Enter the keywords <code>hmac-md5</code> to encrypt the password using MD5.
	password	Assign the interface authentication password.
	level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This setting is the default.
	level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults No default password. **level-1** (if not otherwise specified).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the keywords `level-1` and `level-2`.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.

isis priority

Set the priority of the designated router you select.

Z9500

Syntax `isis priority value [level-1 | level-2]`
To return to the default values, use the `no isis priority [value] [level-1 | level-2]` command.

Parameters

value	This value sets the router priority. The higher the value, the higher the priority. The range is from 0 to 127. The default is 64 .
level-1	(OPTIONAL) Specify the priority for Level 1. This setting is the default.
level-2	(OPTIONAL) Specify the priority for Level 2.

Defaults `value = 64; level-1` (if not otherwise specified).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN is the designated router. Priorities are advertised within hellos. The router with the highest priority becomes the designated intermediate system (DIS).



NOTE: Routers with a priority of 0 cannot be a designated router.

Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address becomes DIS even though its priority is 0.

is-type

Configure IS-IS operating level for a router.

Z9500

Syntax	<code>is-type {level-1 level-1-2 level-2-only}</code> To return to the default values, use the <code>no is-type</code> command.													
Parameters	level-1	Allows a router to act as a Level 1 router.												
	level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This setting is the default.												
	level-2-only	Allows a router to act as a Level 2 router.												
Defaults	level-1-2													
Command Modes	ROUTER ISIS													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.0.2.0	Introduced on the S6000.													
8.3.19.0	Introduced on the S4820T.													
8.3.12.0	Introduced on the S4810.													
8.3.11.1	Introduced on the Z9000.													
Usage Information	The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.													

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. You can configure the IS type as Level 1.

log-adjacency-changes

Generate a log messages for adjacency state changes.

Z9500

Syntax	<code>log-adjacency-changes</code> To disable this function, use the <code>no log-adjacency-changes</code> command.												
Defaults	Adjacency changes are not logged.												
Command Modes	ROUTER ISIS												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></tbody></table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	This command allows you to monitor adjacency state changes, which are useful when you monitor large networks. Messages are logged in the system's error message facility.												

lsp-gen-interval

Set the minimum interval between successive generations of link-state packets (LSPs).

Z9500

Syntax	<code>lsp-gen-interval [level-1 level-2] interval seconds</code> <code>[initial_wait_interval seconds [second_wait_interval seconds]]</code>
---------------	---

To restore default values, use the `no lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

level-1	(OPTIONAL) Enter the keywords <code>level-1</code> to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keywords <code>level-2</code> to apply the configuration to generation of Level-2 LSPs.
<i>interval seconds</i>	Enter the maximum number of seconds between LSP generations. The range is from 0 to 120 seconds. The default is 5 seconds .
<i>initial_wait_interval seconds</i>	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. The range is from 0 to 120 seconds. The default is 1 second .
<i>second_wait_interval seconds</i>	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. The range is from 0 to 120 seconds. The default is 5 seconds .

Defaults

Refer to *Parameters*.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum

wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs this router generates.

Z9500

Syntax	<code>lsp-mtu size</code> To return to the default values, use the <code>no lsp-mtu</code> command.														
Parameters	<table><tr><td>size</td><td>The maximum LSP size, in bytes. The range is from 128 to 1497 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is 1497.</td></tr></table>	size	The maximum LSP size, in bytes. The range is from 128 to 1497 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is 1497 .												
size	The maximum LSP size, in bytes. The range is from 128 to 1497 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is 1497 .														
Defaults	1497 bytes.														
Command Modes	ROUTER ISIS														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>7.5.1.0</td><td>Added support for LSP Throttling Enhancement.</td></tr></table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.5.1.0	Added support for LSP Throttling Enhancement.
Version	Description														
9.5(0.1)	Introduced on the Z9500.														
9.0.2.0	Introduced on the S6000.														
8.3.19.0	Introduced on the S4820T.														
8.3.12.0	Introduced on the S4810.														
8.3.11.1	Introduced on the Z9000.														
7.5.1.0	Added support for LSP Throttling Enhancement.														
Usage Information	The link MTU and the LSP MTU size must be the same. Because each device can generate a maximum of 255 LSPs, consider carefully whether you use the <code>lsp-mtu</code> command.														

lsp-refresh-interval

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their `max-lsp-lifetime` reaches zero and then LSPs is purged.

Z9500

Syntax

lsp-refresh-interval seconds

To restore the default refresh interval, use the no lsp-refresh-interval command.

Parameters

seconds

The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the max-lsp-lifetime command. The range is from 1 to 65535 seconds. The default is 900.

Defaults

900 seconds

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information

The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the max-lsp-lifetime command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization the flooding of refreshed packets causes.

Related Commands

[max-lsp-lifetime](#) — sets the maximum interval that LSPs persist without being refreshed.

max-area-addresses

Configure manual area addresses.

Z9500

Syntax	<code>max-area-addresses number</code> To return to the default values, use the <code>no max-area-addresses</code> command.															
Parameters	<i>number</i>	Set the maximum number of manual area addresses. The range is from 3 to 6. The default is 3 .														
Defaults	3 addresses															
Command Modes	ROUTER ISIS															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>7.5.1.0</td><td>Added support for LSP Throttling Enhancement.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.5.1.0	Added support for LSP Throttling Enhancement.
Version	Description															
9.5(0.1)	Introduced on the Z9500.															
9.0.2.0	Introduced on the S6000.															
8.3.19.0	Introduced on the S4820T.															
8.3.12.0	Introduced on the S4810.															
8.3.11.1	Introduced on the Z9000.															
7.5.1.0	Added support for LSP Throttling Enhancement.															
Usage Information	To configure the number of area addresses on router, use this command. This value must be consistent with routers in the same area, otherwise the router forms only Level 2 adjacencies. The value must be same among all the routers to form Level 1 adjacencies.															

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Z9500

Syntax	<code>max-lsp-lifetime seconds</code> To restore the default time, use the <code>no max-lsp-lifetime</code> command.
--------	---

Parameters	<i>seconds</i>	The maximum lifetime of LSP in seconds. This value must be greater than the <code>lsp-refresh-interval</code> command. The higher the value the longer the LSPs are kept. The range is from 1 to 65535. The default is 1200 .												
Defaults	1200 seconds													
Command Modes	ROUTER ISIS													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.0.2.0	Introduced on the S6000.													
8.3.19.0	Introduced on the S4820T.													
8.3.12.0	Introduced on the S4810.													
8.3.11.1	Introduced on the Z9000.													
Usage Information	Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval. The <code>seconds</code> parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.													
Related Commands	lsp-refresh-interval — sets the link-state packet (LSP) refresh interval.													

maximum-paths

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

Z9500

Syntax	<code>maximum-paths <i>number</i></code> To return to the default values, use the <code>no maximum-paths</code> command.
Parameters	<i>number</i> Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is from 1 to 16. The default is 4 .

Defaults	4																
Command Modes	- ROUTER ISIS (<i>for IPv4</i>) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for multi-topology ISIS.</td></tr> <tr> <td>6.3.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	7.8.1.0	Added support for multi-topology ISIS.	6.3.1.0	Introduced.
Version	Description																
9.5(0.1)	Introduced on the Z9500.																
9.0.2.0	Introduced on the S6000.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Introduced on the S4810.																
8.3.11.1	Introduced on the Z9000.																
7.8.1.0	Added support for multi-topology ISIS.																
6.3.1.0	Introduced.																

metric-style

To generate and accept old-style, new-style, or both styles of type, length, and values (TLV), configure a router.

Z9500

Syntax

```
metric-style {narrow [transition] | transition | wide  
[transition]} [level-1 | level-2]
```

To return to the default values, use the `no metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]` command.

Parameters

narrow	Allows you to generate and accept old-style TLVs. The metric range is from 0 to 63.
transition	Allows you to generate both old-style and new-style TLVs. The metric range is from 0 to 63.
wide	Allows you to generate and accept only new-style TLVs. The metric range is from 0 to 16777215.
level-1	Enables the metric style on Level 1.

	level-2	Enables the metric style on Level 2.												
Defaults	narrow ; if no Level is specified, Level-1 and Level-2 are configured.													
Command Modes	ROUTER ISIS													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.12.0	Introduced on the S4810.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.0.2.0	Introduced on the S6000.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.12.0	Introduced on the S4810.													
Usage Information	If you enter the <code>metric-style wide</code> command, the Dell Networking OS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs. The new-style TLVs have wider metric fields than old-style TLVs.													
Related Commands	isis metric — configures a metric for an interface.													

multi-topology

Enables multi-topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

Z9500

Syntax	<pre>multi-topology [transition]</pre> To return to a single topology configuration, use the <code>no multi-topology [transition]</code> command.
Parameters	transition
Defaults	Disabled

Command Modes	CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Introduced.

net

To configure an IS-IS network entity title (NET) for a routing process, use this mandatory command. If you did not configure a NET, the IS-IS process does not start.

Z9500

Syntax	<pre>net network-entity-title</pre> To remove a net, use the <code>no net network-entity-title</code> command.	
Parameters	<i>network-entity-title</i>	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.
Defaults	Not configured.	
Command Modes	ROUTER ISIS	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

Z9500

Syntax

`passive-interface interface`

To delete a passive interface configuration, use the `no passive-interface interface` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Although the passive interface does not send nor receive routing updates, the network on that interface is still included in the IS-IS updates sent using other interfaces.

redistribute

Redistribute routes from one routing domain to another routing domain.

Z9500

Syntax

```
redistribute {static | connected | rip} [level-1 | level-1-2 |
level-2] [metric metric-value] [metric-type {external |
internal}] [route-map map-name]
```

To end redistribution or disable any of the specified keywords, use the `no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name] command`.

Parameters

connected	Enter the keyword <code>connected</code> to redistribute active routes into IS-IS.
rip	Enter the keyword <code>rip</code> to redistribute RIP routes into IS-IS.
static	Enter the keyword <code>static</code> to redistribute user-configured routes into IS-IS.
metric <i>metric-value</i>	(OPTIONAL) Assign a value to the redistributed route. The range is from 0 to 16777215. The default is 0 . Use a value that is consistent with the destination protocol.
metric-type {external internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following: <code>external</code> <code>internal</code>
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
route-map map-name	(OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routes are imported.

Defaults

- metric metric-value = **0**
- metric-type= internal; **level-2**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added support for IPv6 ISIS.
6.3.1.0	Introduced.

Usage Information

To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command does not affect the state of the other command keywords.

When an LSP with an internal metric is received, the Dell Networking OS considers the route cost while considering the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly are passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow or Transition mode and the metric value in the

`redistribute` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `redistribute` command is advertised.

Related Commands

- [default-information originate](#) — generates a default route for the IS-IS domain.
- [distribute-list out](#) — suppresses networks from being advertised in updates. This command filters redistributed routing information.

redistribute bgp

Redistribute routing information from a BGP process.

Z9500

Syntax

```
redistribute bgp AS number [level-1 | level-1-2 | level-2]
[metric metric-value] [metric-type {external | internal}]
[route-map map-name]
```

To return to the default values, use the `no redistribute bgp` command with the appropriate parameters.

Parameters

<i>AS number</i>	Enter a number that corresponds to the autonomous system number. The range is from 1 to 65355.
<i>level-1</i>	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only.
<i>level-1-2</i>	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
<i>level-2</i>	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This setting is the default.
<i>metric metric-value</i>	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is 0 .
<i>metric-type {external internal}</i>	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • <code>external</code> • <code>internal</code>
<i>route-map map-name</i>	<code>map-name</code> is an identifier for a configured route map. The route map filters imported routes from the source routing protocol to the current routing protocol.

If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults

IS-IS Level 2 routes only

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added support for IPv6 ISIS.
6.3.1.0	Introduced.

Usage Information

BGP to IS-IS redistribution supports “match” options using route maps. You can set the metric value, level, and metric-type of redistributed routes by the redistribution command. You can “set” more advanced options using route maps.

Example

```
FTOS(conf)#router is
FTOS(conf-router_isis)#redistribute bgp 1 level-1 metric 32
metric-type
external route-map rmap-isis-to-bgp
FTOS(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external
route-map
rmap-isis-to-bgp
```

redistribute ospf

Redistribute routing information from an OSPF process.

Z9500

Syntax

```
redistribute ospf process-id [level-1| level-1-2 | level-2]
[match {internal | external}] [metric metric-value] [metric-
type {external | internal}] [route-map map-name]
```

To return to the default values, use the `no redistribute ospf process-id [level-1| level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name]` command.

Parameters	process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.
	metric metric-value	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is 0 .
	metric-type {external internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: - external - internal
	level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
	level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
	level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
	match {external internal}	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are - internal - external
	route-map map-name	map-name is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults	Refer to Parameters.																
Command Modes	- ROUTER ISIS (<i>for IPv4</i>) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.5.1.0</td><td>Added support for IPv6 ISIS.</td></tr> <tr> <td>6.3.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.12.0	Introduced on the S4810.	7.5.1.0	Added support for IPv6 ISIS.	6.3.1.0	Introduced.
Version	Description																
9.5(0.1)	Introduced on the Z9500.																
9.0.2.0	Introduced on the S6000.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.12.0	Introduced on the S4810.																
7.5.1.0	Added support for IPv6 ISIS.																
6.3.1.0	Introduced.																
Usage Information	How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the <code>metric-style</code> command. If the <code>metric-style</code> command is set for Narrow mode and the metric value in the <code>redistribute ospf</code> command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the <code>metric-style</code> command is set for wide mode, the metric value in the <code>redistribute ospf</code> command is advertised.																

router isis

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Z9500

Syntax	<pre>router isis [tag]</pre> To disable IS-IS routing, use the <code>no router isis [tag]</code> command.	
Parameters	tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the <code>tag</code> option is not specified. The tag name must be unique for all IP router processes for a given router.
Defaults	Not configured.	

Command Modes	ROUTER ISIS												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
8.3.11.1	Introduced on the Z9000.												
Usage Information	Configure a network entity title (the <code>net</code> command) to specify the area address and the router system ID. Enable routing on one or more interfaces to establish adjacencies and establish dynamic routing. You can configure only one IS-IS routing process to perform Level 2 routing. A <code>level-1-2</code> designation performs Level 1 and Level 2 routing at the same time.												
Related Commands	• ip router isis — configures IS-IS routing processes for IP on interfaces and attaches an area designator to the routing process. • net — configures an IS-IS network entity title (NET) for a routing process. • is-type — assigns a type for a given area.												

set-overload-bit

To set the overload bit in its non-pseudonode LSPs, configure the router. This setting prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

Z9500

Syntax	<pre>set-overload-bit</pre> To return to the default values, use the <code>no set-overload-bit</code> command.
Defaults	Not set.
Command Modes	• ROUTER ISIS (<i>for IPv4</i>) • CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Added support for multi-topology ISIS.
6.3.1.0	Introduced.

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

Z9500

Syntax

```
show config
```

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

	Version	Description
	8.3.7.1	Introduced on the S4810.
Example (Router-Isis)	The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.	
	<pre> Dell(config-router_isis)#show config ! router isis clns host ISIS 49.0000.0001.F100.E120.0013.00 log-adjacency-changes net 49.0000.0001.F100.E120.0013.00 ! address-family ipv6 unicast maximum-paths 16 multi-topology transition set-overload-bit spf-interval level-1 100 15 20 spf-interval level-2 120 20 25 exit-address-family </pre>	
Example (Address-Family_IPv6)	The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.	
	<pre> Dell(config-router_isis-af_ipv6)#show conf ! address-family ipv6 unicast maximum-paths 16 multi-topology transition set-overload-bit spf-interval level-1 100 15 20 spf-interval level-2 120 20 25 exit-address-family </pre>	

show isis database

Display the IS-IS link state database.

Z9500

Syntax	<pre>show isis database [level-1 level-2] [local] [detail summary] [lspid]</pre>	
Parameters	level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
	level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
	local	(OPTIONAL) Displays local link-state database information.
	detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
	summary	(OPTIONAL) Summary of link-state database information displays when specified.

lspid

(OPTIONAL) Display only the specified LSP.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.1	Introduced on the S4810.

Usage Information

The following describes the `show isis database` command shown in the following example.

Field	Description
IS-IS Level-1/ Level-2 Link State Database	Displays the IS-IS link state database for Level 1 or Level 2.
LSPID	Displays the LSP identifier. The first six octets are the System ID of the originating router. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, the LSP describes system links. If this byte is zero (0), the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP is divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that the system originates an LSP where this command was issued.

Field	Description
LSP Seq Num	This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	This is the checksum of the entire LSP packet.
LSP Holdtime	This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.
ATT	This value represents the Attach bit. This value indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.
P	This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.
OL	This value represents the overload bit, determining congestion. If the overload bit is set, other routers do not use this system as a transit router when calculating routes.

Example

The bold sections identify that MultiTopology IS-IS is enabled.

```
Dell#show isis database
```

```
IS-IS Level-1 Link State Database
LSPID      LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43      580          0/0/0

IS-IS Level-2 Link State Database
LSPID      LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43      580          0/0/0
!
```

```
Dell#show isis database detail ISIS.00-00
```

```
IS-IS Level-1 Link State Database
LSPID      LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002B 0x853B      1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
Metric: 10 IS (MT-IPv6) OSPF.00
  Metric: 10   IP 15.1.1.0 255.255.255.0
Metric: 10 IPv6 (MT-IPv6) 1511::/64
Metric: 10 IPv6 (MT-IPv6) 2511::/64
Metric: 10 IPv6 (MT-IPv6) 1011::/64
  Metric: 10   IPv6 1511::/64
  Metric: 10   IP 10.1.1.0 255.255.255.0
  Hostname: ISIS
```



```

IS-IS Level-2 Link State Database
LSPID      LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002D 0xB2CD      1075          0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
Metric: 10 IS (MT-IPv6) OSPF.00
  Metric: 10   IP 10.1.1.0 255.255.255.0
  Metric: 10   IP 15.1.1.0 255.255.255.0
  Metric: 20   IP 10.3.3.0 255.255.255.0
Metric: 10 IPv6 (MT-IPv6) 1011::/64
Metric: 10 IPv6 (MT-IPv6) 1511::/64
Metric: 10 IPv6 (MT-IPv6) 2511::/64
Metric: 20 IPv6 (MT-IPv6) 1033::/64
  Metric: 10   IPv6 2511::/64
  Metric: 20   IPv6 1033::/64
  Hostname: ISIS

```

show isis graceful-restart detail

Display detailed IS-IS graceful restart related settings.

Z9500

Syntax	<code>show isis graceful-restart detail</code>
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

Example

```

Dell#show isis graceful-restart detail
Configured Timer Value
=====

```

```

Graceful Restart      : Enabled
T3 Timer              : Manual
T3 Timeout Value      : 30
T2 Timeout Value      : 30 (level-1), 30 (level-2)
T1 Timeout Value      : 5, retry count: 1
Adjacency wait time   : 30

Operational Timer Value
=====
Current Mode/State    : Normal/RUNNING
T3 Time left          : 0
T2 Time left          : 0 (level-1), 0 (level-2)
Restart ACK rcv count : 0 (level-1), 0 (level-2)
Restart Req rcv count : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
Database Sync count   : 0 (level-1), 0 (level-2)

```

show isis hostname

Display IS-IS host names configured or learned on the E-Series.

Z9500

Syntax show isis hostname

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Example

```

Dell#show isis hostname
System Id      Dynamic Name Static Name
*F100.E120.0013 Force10      ISIS
Dell#

```

show isis interface

Display detailed IS-IS interface status and configuration information.

Z9500

Syntax	show isis interface [<i>interface</i>]	
Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Command Modes	- EXEC - EXEC Privilege
---------------	---

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example	<pre>Dell>show isis int GigabitEthernet 0/7 is up, line protocol is up MTU 1497, Encapsulation SAP Routing Protocol: IS-IS Circuit Type: Level-1-2 Interface Index 37847070, Local circuit ID 1 Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01 Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10 Number of active level-1 adjacencies: 1 Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01 Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10 Number of active level-2 adjacencies: 1</pre>
---------	--

```

      Next IS-IS LAN Level-1 Hello in 2 seconds
      Next IS-IS LAN Level-2 Hello in 1 seconds
      LSP Interval: 33
GigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
      Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
      Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--

```

show isis neighbors

Display information about neighboring (adjacent) routers.

Z9500

Syntax	<code>show isis neighbors [level-1 level-2] [detail] [<i>interface</i>]</code>	
Parameters	level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
	level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
	detail	(OPTIONAL) Displays detailed information about neighbors.
	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information:
		- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

The following describes the `show isis neighbors` command shown in the following example.

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The range is Up and Init.
Type	This value displays the adjacency type (Layer 2, Layer 2 or both).
Priority	IS-IS priority the neighbor advertises. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Example

The bold sections below identify that Multi-Topology IS-IS is enabled.

```
FTOS#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
FTOS#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
  Adjacency being used for MTs: IPv4 IPv6
FTOS#
```

show isis protocol

Display IS-IS routing information.

Z9500

Syntax `show isis protocol`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example The bold section identifies that Multi-Topology IS-IS is enabled.

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
    49.0000.0001
  Routing for area address(es):
    49.0000.0001
  Interfaces supported by IS-IS:
    GigabitEthernet 1/0 - IP - IPv6
    GigabitEthernet 1/1 - IP - IPv6
    GigabitEthernet 1/10 - IP - IPv6
    Loopback 0 - IP - IPv6
  Redistributing:
  Distance: 115
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
Dell#
```

show isis traffic

This command allows you to display IS-IS traffic interface information.

Z9500

Syntax	<code>show isis traffic [interface]</code>	
Parameters	interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Command Modes	- EXEC - EXEC Privilege
---------------	---

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.
-----------------	---

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information	The following describes the <code>show isis traffic</code> command shown in the following example. <table><tr><th>Item</th><th>Description</th></tr><tr><td>Level-1/Level-2 Hellos (sent/rcvd)</td><td>Displays the number of Hello packets sent and received.</td></tr><tr><td>PTP Hellos (sent/rcvd)</td><td>Displays the number of point-to-point Hellos sent and received.</td></tr></table>	Item	Description	Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.	PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.
Item	Description						
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.						
PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.						

Item	Description
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number of new and refreshed LSPs.
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number of flooded LSPs sent and received.
Level-1/Level-2 LSPs CSNPs (sent/rcvd)	Displays the number of CSNP LSPs sent and received.
Level-1/Level-2 LSPs PSNPs (sent/rcvd)	Displays the number of PSNP LSPs sent and received.
Level-1/Level-2 DR Elections	Displays the number of times designated router elections ran.
Level-1/Level-2 SPF Calculations	Displays the number of shortest path first calculations.
LSP checksum errors received	Displays the number of checksum errors LSPs received.
LSP authentication failures	Displays the number of LSP authentication failures.

Example

```

Dell#sho is traffic
IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
IS-IS: PTP Hellos (sent/rcvd) : 0/0
IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
IS-IS: Level-1 DR Elections : 4
IS-IS: Level-2 DR Elections : 4
IS-IS: Level-1 SPF Calculations : 0
IS-IS: Level-2 SPF Calculations : 389
IS-IS: LSP checksum errors received : 0
IS-IS: LSP authentication failures : 0
Dell#

```


spf-interval

Specify the minimum interval between shortest path first (SPF) calculations.

Z9500

Syntax

```
spf-interval [level-1 | level-2] interval seconds
[initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters	level-1	(OPTIONAL) Enter the keyword <code>level-1</code> to apply the configuration to Level-1 SPF calculations.
	level-2	(OPTIONAL) Enter the keyword <code>level-2</code> to apply the configuration to Level-2 SPF calculations.
	interval seconds	Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is 10 seconds .
	initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. The range is from 0 to 120 seconds. The default is 5 seconds .
	second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. The range is from 0 to 120 seconds. The default is 5 seconds .

Defaults Refer to *Parameters*.

- Command Modes**
- ROUTER ISIS (*for IPv4*)
 - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Added support for multi-topology ISIS.

	Version	Description
	7.5.1.0	Added support for SPF Throttling Enhancement.
Usage Information	This command <code>spf-interval</code> in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using Single Topology mode, use the <code>spf-interval</code> command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations. SPF throttling slows down the frequency at which route calculations are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability. The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (<code>interval seconds</code>). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).	

Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networks's implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs) — known as “port-channels” in the Dell Networking operating software.

 **NOTE:** For static LAG commands, refer to [Port Channel Commands](#) in the [Interfaces](#) chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

clear lacp counters

Clear port channel counters.

Z9500

Syntax	<code>clear lacp port-channel-number counters</code>	
Parameters	<i>port-channel-number</i>	Enter a port-channel number. The range is from 1 to 128.
Defaults	Without a Port Channel specified, the command clears all Port Channel counters.	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.2.1.1	Introduced on the E-Series.

Related Commands [show lacp](#) — displays the LACP configuration.

debug lacp

Debug LACP (configuration, events, and so on).

Z9500

Syntax `debug lacp [config | events | pdu [interface-type [in | out]]]`
 To disable LACP debugging, use the `no [config | events | pdu [interface-type [in | out]]]` command.

Parameters	config	(OPTIONAL) Enter the keyword <code>config</code> to debug the LACP configuration.
	events	(OPTIONAL) Enter the keyword <code>events</code> to debug the LACP event information.
	pdu	(OPTIONAL) Enter the keyword <code>pdu</code> to debug the LACP Protocol Data Unit information.
	<i>interface-type</i> in out	(OPTIONAL) Enter the following keywords and slot/port or number information:
		- For a Ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. Optionally, enter an <code>in</code> or <code>out</code> parameter: - Receive enter <code>in</code> - Transmit enter <code>out</code>

Defaults none

- Command Modes**
- EXEC
 - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

Z9500

Syntax `lacp long-timeout`
 To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.

Defaults **1 second**

Command Modes INTERFACE (conf-if-po-number)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.
Related Commands	show lacp — displays the LACP configuration.

lacp port-priority

To influence which ports will be put in Standby mode when there is a hardware limitation that prevents all compatible ports from aggregating, configure the port priority.

Z9500

Syntax	<code>lacp port-priority <i>priority-value</i></code> To return to the default setting, use the <code>no lacp port-priority <i>priority-value</i></code> command.
--------	--

Parameters	<i>priority-value</i> Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is 32768.
------------	--

Defaults	32768
----------	--------------

Command Modes	INTERFACE
---------------	-----------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

lacp system-priority

Configure the LACP system priority.

Z9500

Syntax	lacp system-priority <i>priority-value</i>	
Parameters	<i>priority-value</i>	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is 32768 .
Defaults	32768	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

port-channel mode

Configure the LACP port channel mode.

Z9500

Syntax	port-channel <i>number</i> mode [active] [passive] [off]	
Parameters	<i>number</i>	Enter the keywords <i>number</i> then a number.
	<i>active</i>	Enter the keyword <i>active</i> to set the mode to the active state.

		 NOTE: LACP modes are defined in <i>Usage Information</i> .												
	passive	Enter the keyword <code>passive</code> to set the mode to the passive state.												
		 NOTE: LACP modes are defined in <i>Usage Information</i> .												
	off	Enter the keyword <code>off</code> to set the mode to the off state.												
		 NOTE: LACP modes are defined in <i>Usage Information</i> .												
Defaults	off													
Command Modes	INTERFACE													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.11.1	Introduced on the Z9000.													
7.6.1.0	Introduced on the S-Series.													
7.5.1.0	Introduced on the C-Series.													
6.2.1.1	Introduced on the E-Series.													
Usage Information	LACP Modes													
	Mode	Function												
	active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.												
	passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets												
	off	An interface cannot be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.												

port-channel-protocol lacp

Enable LACP on any LAN port.

Z9500

Syntax	port-channel-protocol lacp To disable LACP on a LAN port, use the <code>no port-channel-protocol lacp</code> command.												
Command Modes	INTERFACE												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	6.2.1.1	Introduced on the E-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
6.2.1.1	Introduced on the E-Series.												
Related Commands	show lacp — displays the LACP information. show interfaces port-channel — displays information on configured Port Channel groups.												

show lacp

Display the LACP matrix.

Z9500

Syntax	show lacp port-channel-number [sys-id counters]	
Parameters	port-channel-number sys-id	Enter a port-channel number. The range is from 1 to 128. (OPTIONAL) Enter the keywords <code>sys-id</code> and the value that identifies a system.

	counters	(OPTIONAL) Enter the keyword <code>counters</code> to display the LACP counters.
Defaults	Without a Port Channel specified, the command clears all Port Channel counters.	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example (Port-Channel-Number)

```
Dell#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID:Priority 32768, Address 0001.e800.a12b
Partner System ID:Priority 32768, Address 0001.e801.45a5
        Actor Admin Key 1, Oper Key 1, Partner Oper
Key 1
        LACP LAG 1 is an aggregatable link

A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-
OUT_OF_SYNC
I-Collection enabled, J-Collection disabled, K-Distribution
enabled L-Distribution disabled,
M-Partner Defaulted, N-Partner Non-defaulted, O-Receiver is in
expired state,
P-Receiver is not in expired state

Port Te 1/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1   Priority 128
        Oper: State ACEGIKNP Key 1   Priority 128
  Partner Admin: State BDFHJLMP Key 0   Priority 0
        Oper: State BCEGIKNP Key 1   Priority 128
Dell#
```

Example (Sys-id)

```
Dell#show lacp 1 sys-id
Actor   System ID: Priority 32768, Address 0001.e800.a12b
Partner System ID: Priority 32768, Address 0001.e801.45a5

Dell#
```

**Example
(Counter)**

```
Dell#show lacp 1 counters
-----
          LACP PDU      Marker PDU      Unknown      Illegal
Port      Xmit Recv      Xmit Recv      Pkts Rx      Pkts Rx
-----
Te 1/6    200   200        0     0          0          0
Dell#
```

**Related
Commands**

[clear lacp counters](#) — clears the LACP counters.

[show interfaces port-channel](#) — displays information on configured Port Channel groups.

Layer 2

This chapter describes commands to configure Layer 2 features.
This chapter contains the following sections:

- [MAC Addressing Commands](#)
- [Virtual LAN \(VLAN\) Commands](#)
- [Far-End Failure Detection \(FEFD\)](#)

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

clear mac-address-table

Clear the MAC address table of all MAC address learned dynamically.

Z9500

Syntax	<pre>clear mac-address-table {dynamic sticky }{address <i>mac-address</i> all interface <i>interface</i> vlan <i>vlan-id</i>}</pre>	
Parameters	dynamic	Enter the keyword <code>dynamic</code> to specify dynamically-learned MAC addresses.
	sticky	Enter the keyword <code>sticky</code> to specify sticky MAC addresses.
	address <i>mac-address</i>	Enter the keyword <code>address</code> then a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
	all	Enter the keyword <code>all</code> to delete all MAC address entries in the MAC address table.
	interface <i>interface</i>	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	vlan <i>vlan-id</i>	Enter the keyword <code>vlan</code> then a VLAN ID number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added support for sticky MAC addresses.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

Z9500

Syntax

`mac-address-table aging-time seconds`

Parameters

seconds Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter 0. The range is from 10 to 1000000. The default is **1800 seconds**.

Defaults

1800 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	On the E-Series, available in INTERFACE VLAN context, reduced the minimum aging time in the INTERFACE VLAN context from 10 seconds to 1 second.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

[mac learning-limit](#) — sets the MAC address learning limits for a selected interface.

[show mac-address-table aging-time](#) — displays the MAC aging time.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and VLANs.

Z9500

Syntax

```
mac-address-table static mac-address {multicast vlan vlan-id
output-range interface}{output interface vlan vlan-id}
```

To remove a MAC address, use the `no mac-address-table static mac-address output interface vlan vlan-id` command.

Parameters

<i>mac-address</i>	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
<i>multicast</i>	Enter a vlan port to where L2 multicast MAC traffic is forwarded.
	 NOTE: Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.
<i>output interface</i>	For a unicast MAC address, enter the keyword <code>output</code> then one of the following interfaces for which traffic is forwarded: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
<i>output-range interface</i>	For a multicast MAC address, enter the keyword <code>output-range</code> then one of the following interfaces to indicate a range of ports for which traffic is forwarded:

	- For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.																				
	vlan <i>vlan-id</i> Enter the keyword <code>vlan</code> then a VLAN ID number from 1 to 4094.																				
Defaults	Not configured.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Added support for output range parameter for S4810 and Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Added support for output range parameter for S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
9.1(0.0)	Added support for output range parameter for S4810 and Z9000.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																				
8.3.7.0	Introduced on the S4810.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.2.1.1	Introduced on the E-Series.																				
Example (Unicast)	<pre>mac-address-table static 00:01:00:00:00:01 {output Te 0/2 vlan 2}</pre>																				
Example (Multicast)	<pre>mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output-range Te 0/2,Te 0/3}</pre>																				
Related Commands	show mac-address-table — displays the MAC address table.																				

mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

Z9500

Syntax `[no] mac-address-table station-move refresh-arp`

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information For details about using this command, refer to the “NIC Teaming” section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide*.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

Z9500

Syntax `mac learning-limit address_limit [vlan vlan-id] [station-move-violation [dynamic]] [dynamic [no-station-move| station-move]]`

Parameters

<i>address_limit</i>	Enter the maximum number of MAC addresses that can be learned on the interface. The range is from 1 to 1000000.
<i>vlan vlan-id</i>	E-Series only: Enter the keyword then the VLAN ID. The range is from 1 to 4094.
<i>dynamic</i>	(OPTIONAL) Enter the keyword <code>dynamic</code> to allow aging of MACs even though a learning limit is configured.

station-move-violation (OPTIONAL) Enter the keywords `station-move` to allow a station move on learned MAC addresses.

Defaults

- On S-Series, the default behavior is dynamic.



NOTE: "Static" means manually entered addresses, which do not age.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Deprecated the <code>no-station-move</code> command (replaced by the <code>mac-learning-limit mac-address-sticky</code> command).
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.
8.2.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added the <code>station-move</code> option.
6.5.1.0	Added support for MAC Learning-Limit on the LAG.

Usage Information

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If you do not specify the `vlan` option, the MAC address counters are not VLAN-based. That is, the sum of the addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning limit.

MAC Learning Limit violation logs and actions are not available on a per-VLAN basis.

With the keyword `no-station-move` option, MAC addresses learned through this feature on the selected interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no effect on already learned MAC addresses.

After the MAC address learning limit is reached, the MAC addresses do not age out unless you add the `dynamic` option. To clear statistics on MAC address learning, use the `clear counters` command with the `learning-limit` parameter.



NOTE: If you configure this command on an interface in a routed VLAN, and after the MAC addresses learned reaches the limit set in the `mac learning-limit` command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

[clear counters](#) — Clear counters used in the `show interface` command.

[clear mac-address-table](#) — clears the MAC address table of all MAC address learned dynamically.

[mac learning-limit mac-address-sticky](#) — Replaces deprecated `no-station-move` parameter.

[show mac learning-limit](#) — displays MAC learning-limit configuration.

mac learning-limit learn-limit-violation

Configure an action for a MAC address learning-limit violation.

Z9500

Syntax

```
mac learning-limit learn-limit-violation {log | shutdown}
```

To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.

Parameters

- | | |
|-----------------|--|
| log | Enter the keyword <code>log</code> to generate a syslog message on a learning-limit violation. |
| shutdown | Enter the keyword <code>shutdown</code> to shut down the port on a learning-limit violation. |

Defaults

none

Command Modes

INTERFACE (conf-if-interface-slot/port)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information	This command is supported on physical interfaces, static LAGs, and LACP LAGs.
Related Commands	show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit mac-address-sticky

Maintain the dynamically learned mac addresses as sticky MAC addresses on the selected port.

Z9500

Syntax	<code>mac learning-limit mac-address-sticky</code> To convert the sticky MAC addresses to dynamic MAC addresses, use the <code>no mac learning-limit</code> command.	
Parameters	<i>mac-address-sticky</i>	Configures the dynamic MAC addresses as sticky on an interface.
Defaults	none	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information	If you configure <code>mac-learning-limit</code> and the sticky MAC feature is enabled, dynamically learned MAC addresses are converted to sticky for that port. Any new MAC address that is learned also becomes sticky for that port.
Related Commands	show mac learning-limit — displays the details of the mac learning-limit.

mac learning-limit station-move-violation

Specify the actions for a station move violation.

Z9500

Syntax	<code>mac learning-limit station-move-violation {log shutdown-both shutdown-offending shutdown-original}</code> To disable a configuration, use the <code>no mac learning-limit station-move-violation</code> command, then the configured keyword.
---------------	--

Parameters	log	Enter the keyword <code>log</code> to generate a syslog message on a station move violation.
	shutdown-both	Enter the keyword <code>shutdown</code> to shut down both the original and offending interface and generate a syslog message.
	shutdown-offending	Enter the keywords <code>shutdown-offending</code> to shut down the offending interface and generate a syslog message.
	shutdown-original	Enter the keywords <code>shutdown-original</code> to shut down the original interface and generate a syslog message.

Defaults	none
-----------------	------

Command Modes	INTERFACE (conf-if-interface-slot/port)
----------------------	---

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information	This command is supported on physical interfaces, static LAGs, and LACP LAGs.
Related Commands	show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit reset

Reset the MAC address learning-limit error-disabled state.

Z9500

Syntax	<code>mac learning-limit reset</code>
Defaults	none
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

show cam mac linecard (dynamic or static)

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Z9500

Syntax	<pre>show cam mac linecard slot-id port-set port-pipe [address mac_addr dynamic interface interface static vlan vlan-id]</pre>	
Parameters	linecard slot-id	(REQUIRED) Enter the keyword <code>linecard</code> then a slot number to select the linecard for which to gather information. The range of Z9500 slot IDs are from 0 to 2.

port-set <i>port-pipe</i>	(REQUIRED) Enter the keywords <code>port-set</code> then a port-pipe number to specify the port pipe for which to gather information. The range of port pipe numbers is from 0 to 3.
address <i>mac-addr</i>	(OPTIONAL) Enter the keyword <code>address</code> then a MAC address in the <code>nn:nn:nn:nn:nn:nn</code> format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword <code>dynamic</code> to display only those MAC addresses the switch dynamically learns.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> then the interface type, slot and port information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
static	(OPTIONAL) Enter the keyword <code>static</code> to display only those MAC addresses specifically configured on the switch.
vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell# show cam mac linecard 1 port-set 0
PVlanId    Mac Address      Region    Interface
1          00:01:02:03:04:09  DYNAMIC   Fo 2/0
0          74:86:7a:ff:6f:1c  LOCAL DA  00001
1          00:11:22:33:44:55  STATIC    Fo 2/8
```

1	00:01:02:03:04:07	DYNAMIC	Fo 2/0
1	00:01:02:03:04:08	DYNAMIC	Fo 2/0
0	ff:ff:ff:ff:ff:ff	STATIC	00001
1	00:01:02:03:04:05	DYNAMIC	Fo 2/0
1	00:01:02:03:04:06	DYNAMIC	Fo 2/0

show mac-address-table

Display the MAC address table.

Z9500

Syntax

```
show mac-address-table [address mac-address | interface
interface | vlan vlan-id] [aging-time] [dynamic | static]
[count [vlan vlan-id] [interface interface-type [slot [/
port]]]]
```

Parameters

address <i>mac-address</i>	(OPTIONAL) Enter the keyword <i>address</i> then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword <i>dynamic</i> to display only those MAC addresses the switch dynamically learns. Optionally, you can also add one of these combinations: <i>address/mac-address</i> , <i>interface/interface</i> , or <i>vlan vlan-id</i> .
static	(OPTIONAL) Enter the keyword <i>static</i> to display only those MAC addresses specifically configured on the switch. Optionally, you can also add one of these combinations: <i>address/mac-address</i> , <i>interface/interface</i> , or <i>vlan vlan-id</i> .
aging-time	Enter the keyword <i>aging-time</i> to display only aging-time information.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <i>interface</i> then the interface type, slot and port information: - For a Port Channel interface, enter the keywords <i>port-channel</i> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <i>TenGigabitEthernet</i> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <i>fortyGigE</i> then the slot/port information.
interface <i>interface-type</i>	(OPTIONAL) Instead of entering the keyword <i>interface</i> then the interface type, slot and port information, as above, you can enter the interface type, then just a slot number.
vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <i>vlan</i> then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

count (OPTIONAL) Enter the keyword `count`, then optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Updated the output.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • po — Port Channel then a number. The range is from 1 to 255 for TeraScale. • te — 10-Gigabit Ethernet then a slot/port. • fo — 40-Gigabit Ethernet then a slot/port.

Column Heading	Description
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

Example

```
Dell(conf)#do show mac-address-table
Codes: *N - VLT Peer Synced MAC
VlanId    Mac
Address    Type          Interface    State
2          00:00:00:00:00:01    Dynamic (N)    Po
128        Active
2          00:00:00:00:00:02    Dynamic (N)    Po
10         Active
2          00:00:00:00:00:03    Dynamic        Po
100        Active
2          00:00:00:00:00:04    Dynamic        Po
10         Active
```

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned (Dynamic), or associated with a specific port (Sticky). An (N) indicates that the specified MAC address has been learnt by a neighbor and is synced to the node.
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: - po — Port Channel followed by a number. Range for Terascale is from 1 to 255. \ - te — 10-Gigabit Ethernet followed by a slot/port. - fo — 40-Gigabit Ethernet then a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

The following describes the `show mac-address-table count` command shown in the following example.

Line Beginning With	Description
MAC Entries...	Displays the number of MAC entries learned per VLAN.
Dynamic Address...	Lists the number of dynamically learned MAC addresses.
Static Address...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses the switch uses.

**Example
(Count)**

```
Dell# show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :      110
Static Address (User-defined) Count : 0
Sticky Address Count :      0
Total Synced Mac from Peer(N): 100
Total MAC Addresses in Use:  110
Dell#
```

**Related
Commands**

[show mac-address-table aging-time](#) — displays MAC aging time.

show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

Z9500

Syntax

```
show mac-address-table aging-time [vlan vlan-id]
```

Parameters

vlan *vlan-id* (OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.
7.7.1.0	Introduced on the C-Series and S-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#show mac-address-table aging-time
Mac-address-table aging time : 1800
Dell#
```

Related
Commands

[show mac-address-table](#) — displays the current MAC address configuration.

show mac learning-limit

Display MAC address learning limits set for various interfaces.

Z9500

Syntax

```
show mac learning-limit [violate-action] [detail] [interface  
interface]
```

Parameters

- | | |
|--------------------------------|---|
| violate-action | (OPTIONAL) Enter the keywords <code>violate-action</code> to display the MAC learning limit violation status. |
| detail | (OPTIONAL) Enter the keyword <code>detail</code> to display the MAC learning limit in detail. |
| interface
interface | (OPTIONAL) Enter the keyword <code>interface</code> with the following keywords and slot/port or number information: <ul style="list-style-type: none">• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. |

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.5.1.0	Added support for the <code>violate-action</code> and <code>detail</code> options.
6.5.1.0	Added support for Port Channel.

Example

```
Dell#show mac learning-limit
Interface Learning Dynamic Static Unknown SA
Slot/port Limit MAC count MAC count Drops
Te 1/0 10 0 0 0
Te 1/1 5 0 0 0
Dell#show mac learning-limit interface gig 1/0
Interface Learning Dynamic Static Unknown SA
Slot/port Limit MAC count MAC count Drops
Te 1/0 10 0 0 0
```

Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

 **NOTE:** For more information, refer to [VLAN Stacking](#) and VLAN-related commands, such as [portmode hybrid](#) in the [Interfaces](#) chapter.

default vlan-id

Specify a VLAN as the Default VLAN.

Z9500

Syntax

```
default vlan-id vlan-id
```

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id vlan-id` syntax.

Parameters

vlan-id Enter the VLAN ID number of the VLAN to become the new Default VLAN. The range is from 1 to 4094. The default is **1**.

Defaults

The Default VLAN is VLAN **1**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

**Usage
Information**

To return VLAN 1 as the Default VLAN, use this command syntax (`default-vlan-id 1`).

The Default VLAN contains only untagged interfaces.

**Related
Commands**

[interface vlan](#) — configures a VLAN.

default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

Z9500

Defaults

Enabled.

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced

Usage Information The `no default vlan disable` command is not listed in the running-configuration, but when the default VLAN is disabled, `default-vlan disable` is listed in the running-configuration.

name

Assign a name to the VLAN.

Z9500

Syntax `name vlan-name`
To remove the name from the VLAN, use the `no name` command.

Parameters ***vlan-name*** Enter up to 32 characters as the name of the VLAN.

Defaults Not configured.

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information To display information about a named VLAN, enter the `show vlan` command with the name parameter or the `show interfaces description` command.

Related Commands [interface vlan](#) — configures a VLAN.

[show vlan](#) — displays the current VLAN configurations on the switch.

show config

Display the current configuration of the selected VLAN.

Z9500

Syntax	<code>show config</code>
Command Modes	INTERFACE VLAN
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-if-vl-100)#show config
!
interface Vlan 100
  no ip address
  no shutdown
Dell(conf-if-vl-100)#
```

show vlan

Display the current VLAN configurations on the switch.

Z9500

Syntax	<code>show vlan [brief id <i>vlan-id</i> name <i>vlan-name</i>]</code>	
Parameters	brief	(OPTIONAL) Enter the keyword <code>brief</code> to display the following information: • VLAN ID • VLAN name (left blank if none is configured) • Spanning Tree Group ID • MAC address aging time

- IP address

id *vlan-id* (OPTIONAL) Enter the keyword `id` and VLAN ID number from 1 to 4094 to display the configuration of the specified VLAN.

name *vlan-name* (OPTIONAL) Enter the keyword `name` and the name assigned to a VLAN. Only information on the specified VLAN is displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Updated to support OpenFlow.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Augmented to display PVLAN data for the C-Series and S-Series and revised the output to include the Description field to display a user-entered VLAN description.
7.6.1.0	Introduced on the S-Series and revised the output to display Native VLAN.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show vlan` command shown in the following example.

Column Heading	Description
(Column 1 — no heading)	• asterisk symbol (*) = Default VLAN • G = GVRP VLAN • P = primary VLAN • C = community VLAN • I = isolated VLAN • O = OpenFlow

Column Heading	Description
NUM	Displays existing VLAN IDs.
Status	Displays the word <i>Inactive</i> for inactive VLANs and the word <i>Active</i> for active VLANs.
Q	• Displays G for GVRP tagged • M for member of a VLAN-Stack VLAN • T for tagged interface • U for untagged interface • x (not capitalized x) for Dot1x untagged • X (capitalized X) for Dot1x tagged • o (not capitalized o) for OpenFlow untagged • O (capitalized O) for OpenFlow tagged • H for VSN tagged • i (not capitalized i) for Internal untagged • I (capitalized I) for Internal tagged • v (not capitalized v) for VLT untagged • V (capitalized V) for VLT tagged
Ports	Displays the type, slot, and port information. • Po = port channel • Te = 10-Gigabit Ethernet • Fo = 40-Gigabit Ethernet

Example

```
Dell#show vlan
```

```
Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring VLANs, P - Primary, C - Community, I - Isolated
       O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged
```

NUM	Status	Description	Q	Ports
* 1	Active		U	Fo 0/0
10	Active		U	Fo 2/8
0/140,Te 1/80)			T	Po10 (Te
1/81)			T	Po20 (Te
20	Active		T	Po10 (Te
0/140,Te 1/80)			T	Po20 (Te
1/81)			T	Po20 (Te
30	Active		T	Fo 2/0

Example (VLAN ID)

```
Dell# show vlan id 20

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring VLANs, P - Primary, C - Community, I - Isolated
O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged

      NUM      Status      Description      Q Ports
      20      Active
0/140,Te 1/80)
                                     T Po10(Te
                                     T Po20(Te
                                     T Fo 2/0
```

Example (Brief)

```
Dell#show vlan brief

VLAN Name      STG   MAC Aging IP
Address
-----
1
unassigned
10
unassigned
20
2.3.3.3/24
30
2.1.1.1/24
0      1800
0      1800
0      1800
0      1800
```

Example (Name)

```
Dellconf)#interface vlan 20
Dell(conf-if-vl-20)#name test
Dell(conf-if-vl-20)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port
Mirroring VLANs, P - Primary, C - Community, I - Isolated
O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT
untagged, V - VLT tagged

      NUM      Status      Description      Q Ports
      20      Active
0/140,Te 1/80)
                                     T Po10(Te
                                     T Po20(Te
                                     T Fo 2/0
```

Related Commands

[interface vlan](#) — configures a VLAN.

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

Z9500

Syntax	<code>tagged interface</code> To remove a tagged interface from a VLAN, use the <code>no tagged interface</code> command.																			
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.																		
Defaults	All interfaces in Layer 2 mode are untagged.																			
Command Modes	INTERFACE VLAN																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																			
8.3.7.0	Introduced on the S4810.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.2.1.1	Introduced on the E-Series.																			
Usage Information	When you use the <code>no tagged</code> command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, remove it from all VLANs to change it to an untagged interface.																			

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

**Related
Commands**

[interface vlan](#) — configures a VLAN.

[untagged](#) — specifies which interfaces in a VLAN are untagged.

track ip

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

Z9500

Syntax

```
track ip interface
```

To remove the tracking feature from the VLAN, use the `no track ip interface` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

**Command
Modes**

INTERFACE VLAN

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	6.2.1.1	Introduced on the E-Series.
Version	Description				
6.2.1.1	Introduced on the E-Series.				
Usage Information	When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the <code>track ip</code> command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP. If the <code>track ip</code> command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN. The Layer 2 state of the VLAN, and hence the Layer 2 traffic, is not affected by the <code>track ip</code> command configuration.				
Related Commands	interface vlan — configures a VLAN. tagged — specifies which interfaces in a VLAN are tagged.				

untagged

Add a Layer 2 interface to a VLAN as an untagged interface.

Z9500

Syntax	<pre>untagged interface</pre> To remove an untagged interface from a VLAN, use the <code>no untagged interface</code> command.		
Parameters	<table> <tr> <td><i>interface</i></td><td> Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. </td></tr> </table>	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.		
Defaults	All interfaces in Layer 2 mode are untagged.		
Command Modes	INTERFACE VLAN		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.		

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
	8.3.7.0	Introduced on the S4810.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Usage Information	Untagged interfaces can only belong to one VLAN.	
	In the Default VLAN, you cannot use the <code>no untagged interface</code> command. To remove an untagged interface from all VLANs, including the Default VLAN, enter INTERFACE mode and use the <code>no switchport</code> command.	
Related Commands	interface vlan — configures a VLAN.	
	tagged — specifies which interfaces in a VLAN are tagged.	

Far-End Failure Detection (FEFD)

The Dell Networking operating software supports far-end failure detection (FEFD) on the Ethernet interfaces.

The FEFD feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- During an RPM failover, FEFD is operationally disabled for approximately 8 to 10 seconds.
- By default, FEFD is disabled.

debug fefd

Enable debugging of FEFD.

Z9500

Syntax

```
debug fefd {events | packets} [interface]
```

To disable debugging of FEFD, use the `no debug fefd {events | packets} [interface]` command.

Parameters

events

Enter the keyword `events` to enable debugging of FEFD state changes.

	packets	Enter the keyword <code>packets</code> to enable debugging of FEFD to view information on packets sent and received.
	interface	(OPTIONAL) Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/ port information.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.12.0	Introduced on the S4810.
Related Commands	fe fd — enables far-end failure detection on an interface. fe fd reset — enables FEFD globally on the system.	

fe fd

Enable Far-End Failure Detection on an interface, set the FEFD interval, or select the FEFD mode.

Z9500

Syntax	<code>fe fd {disable interval mode {aggressive normal}}</code>	
Parameters	disable	Enter the keyword disable to disable FEFD for the specified interface.
	interval	Enter the keyword interval , followed by a value to specify the FEFD interval in seconds. Range is from 3 to 300. Default is 15.
	mode	Enter the keyword mode followed by the mode type to specify the FEFD mode. normal: Change the link state to “unknown” when a far-end failure is detected by the software on that interface. When the interface is placed in an “unknown” state, the software brings down the line protocol.

- **aggressive:** Change the link state to “error-disabled” when a far-end failure is detected by the software on that interface. When an interface is placed in an “error-disabled” state, you must enter the `fehd reset` command to reset the interface state. Range is normal or aggressive. Default is normal.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information When you enter `no fehd` for an interface and `fehd-global`, FEFD is enabled on the interface because the `no fehd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fehd reset` command.

Related Commands

- [fehd disable](#) — disables far-end failure detection on an interface.
- [fehd reset](#) — enables FEFD globally on the system.
- [fehd mode](#) — changes FEFD mode on an interface.

fehd disable

Disable FEFD on an interface only. This command overrides the `fehd reset` command for the interface.

Z9500

Syntax `fehd disable`
To re-enable FEFD on an interface, use the `no fehd disable` command.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

When you enter `no fefd` for an interface and `fefd-global`, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd reset` command.

Related Commands

- [fefd reset](#) — enables FEFD globally on the system.
- [fefd mode](#) — changes FEFD mode on an interface.

fefd interval

Set an interval between control packets.

Z9500

Syntax

`fefd interval seconds`

To return to the default value, use the `no fefd interval` command.

Parameters

seconds

Enter a number as the time between FEFD control packets. The range is from 3 to 300 seconds. The default is **15 seconds**.

Defaults

15 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related
Commands

- [fefd](#) — enables far-end failure detection.

fefd mode

Change the FEFD mode on an interface.

Z9500

Syntax

`fefd mode {normal | aggressive}}`

To return the FEFD mode to the default of normal, use the `no fefd mode` command.

Parameters

- | | |
|-------------------|---|
| normal | (OPTIONAL) Enter the keyword <code>normal</code> to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. |
| aggressive | (OPTIONAL) Enter the keyword <code>aggressive</code> to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, enter the <code>fefd reset</code> command to reset the interface state. |

Defaults

normal

**Command
Modes**

INTERFACE

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related
Commands

- [fefd](#) — enables far-end failure detection.

fefd reset

Reset all interfaces or a single interface that was in "error-disabled" mode.

Z9500

Syntax	fefd reset [<i>interface</i>]											
Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/ port information.										
Defaults	Not configured.											
Command Modes	EXEC Privilege											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.12.0	Introduced on the S4810.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.19.0	Introduced on the S4820T.											
8.3.11.1	Introduced on the Z9000.											
8.3.12.0	Introduced on the S4810.											
Related Commands	fefd — enables far-end failure detection.											

fefd-global interval

Configure an interval between FEFD control packets.

Z9500

Syntax	<code>fefd-global interval seconds</code> To return to the default value, use the <code>no fefd-global interval</code> command.	
Parameters	<i>seconds</i>	Enter a number as the time between FEFD control packets. The range is from 3 to 300 seconds. The default is 15 seconds .

Defaults	15 seconds										
Command Modes	CONFIGURATION										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										
Related Commands	• fefd — enables far-end failure detection. • fefd-global — enables FEFD globally on the system.										

fefd-global

Enable FEFD globally on the system.

Z9500

Syntax	<pre>fefd-global [interval seconds][mode {normal aggressive}]</pre> To disable FEFD globally, use the <code>no fefd-global [mode {normal aggressive}]</code> command.						
Parameters	<table><tr><td>interval <i>seconds</i></td><td>Enter the keyword <code>interval</code> followed by the number of seconds to wait between FEFD control packets. Range is from 3 to 300 seconds. Default is 15 seconds.</td></tr><tr><td>normal</td><td>(OPTIONAL) Enter the keywords <code>mode normal</code> to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. The default is Normal mode.</td></tr><tr><td>aggressive</td><td>(OPTIONAL) Enter the keywords <code>mode aggressive</code> to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, t enter the <code>fefd reset</code> command to reset the interface state.</td></tr></table>	interval <i>seconds</i>	Enter the keyword <code>interval</code> followed by the number of seconds to wait between FEFD control packets. Range is from 3 to 300 seconds. Default is 15 seconds.	normal	(OPTIONAL) Enter the keywords <code>mode normal</code> to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. The default is Normal mode .	aggressive	(OPTIONAL) Enter the keywords <code>mode aggressive</code> to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, t enter the <code>fefd reset</code> command to reset the interface state.
interval <i>seconds</i>	Enter the keyword <code>interval</code> followed by the number of seconds to wait between FEFD control packets. Range is from 3 to 300 seconds. Default is 15 seconds.						
normal	(OPTIONAL) Enter the keywords <code>mode normal</code> to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. The default is Normal mode .						
aggressive	(OPTIONAL) Enter the keywords <code>mode aggressive</code> to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, t enter the <code>fefd reset</code> command to reset the interface state.						
Defaults	Disabled.						

Command Modes	CONFIGURATION										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.12.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.12.0	Introduced on the S4810.										
Usage Information	If you enter only the <code>fezd-global</code> syntax, the mode is normal and the default interval is 15 seconds. If you disable FEFD globally (<code>no fezd-global</code>), the system does not remove the FEFD interface configuration.										
Related Commands	• fezd — enables far-end failure detection. • fezd-global interval — configures an interval between FEFD control packets. • show fezd — shows the FEFD command output.										

show fezd

View FEFD status globally or on a specific interface.

Z9500

Syntax	<code>show fezd [interface]</code>
Parameters	<i>interface</i> (OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/ port information.
Command Modes	• EXEC • EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fefd` command shown in the following example.

Field	Description
Interface	Displays the interfaces type and number.
Mode	Displays the mode (aggressive or normal) or NA if the interface contains <code>fefd reset</code> in its configuration.
Interval	Displays the interval between FEFD packets.
State	Displays the state of the interface and can be one of the following: • bi-directional (interface is up, connected and hearing neighbor's echoes). • err-disabled (only found when FEFD mode is aggressive and when the interface has not hearing its neighbor's echoes for three times the message interval. To reset an interface in this state, use the <code>fefd reset</code> command.) • unknown (only found when FEFD mode is normal). • locally disabled (interface contains the <code>fefd reset</code> command in its configuration). • Admin Shutdown (interface is disabled with the <code>shutdown</code> command).

Example

```
Dell#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is
'Aggressive'.
```

INTERFACE	MODE	INTERVAL (second)	STATE
Te 1/0	Aggressive	10	Admin Shutdown
Te 1/1	Aggressive	10	Admin Shutdown
Te 1/2	Aggressive	10	Admin Shutdown
Te 1/3	Aggressive	10	Admin Shutdown
Te 1/4	Aggressive	10	Admin Shutdown
Te 1/5	Aggressive	10	Admin Shutdown
Te 1/6	Aggressive	10	Admin Shutdown
Te 1/7	Aggressive	10	Admin Shutdown
Te 1/8	Aggressive	10	Admin Shutdown
Te 1/9	Aggressive	10	Admin Shutdown
Te 1/10	NA	NA	Locally disabled
Te 1/11	Aggressive	10	Err-disabled

```
Dell#
```

**Related
Commands**

- [fehd](#) — enables far-end failure detection.
- [fehd disable](#) — disables FEFD on an interface only.
- [fehd-global](#) — enables FEFD globally on the system.
- [fehd reset](#) — resets all interfaces or a single interface that was in “error-disabled” mode.

Link Layer Discovery Protocol (LLDP)

Link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.

This chapter contains the following sections:

- [LLPD Commands](#)
- [LLDP-MED Commands](#)

LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating system implementation of LLDP is based on IEEE standard 801.1ab.

The starting point for using LLDP is invoking LLDP with the `protocol lldp` command in either CONFIGURATION or INTERFACE mode.

The information LLDP distributes is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

LLPD Commands

The following are LLDP commands.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

Z9500

Syntax `advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}`

To remove advertised dot1-tlv, use the `no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}` command.

Parameters	port-protocol-vlan-id	Enter the keywords <code>port-protocol-vlan-id</code> to advertise the port protocol VLAN identification TLV.
	port-vlan-id	Enter the keywords <code>port-vlan-id</code> to advertise the port VLAN identification TLV.
	vlan-name	Enter the keywords <code>vlan-name</code> to advertise the vlan-name TLV. This keyword is only supported on the C-Series and S-Series.

Defaults	Disabled.																
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if- <i>interface</i> -lldp)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series. Added the <code>vlan-name</code> option.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Introduced on the S-Series. Added the <code>vlan-name</code> option.	7.6.1.0	Introduced on the C-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.7.1.0	Introduced on the S-Series. Added the <code>vlan-name</code> option.																
7.6.1.0	Introduced on the C-Series.																
7.4.1.0	Introduced on the E-Series.																
Related Commands	protocol lldp (Configuration) — enables LLDP globally. debug lldp interface — debugs LLDP. show lldp neighbors — displays the LLDP neighbors. show running-config lldp — displays the LLDP running configuration.																

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

Z9500

Syntax	<pre>advertise dot3-tlv {max-frame-size}</pre> To remove advertised dot3-tlv, use the <code>no advertise dot3-tlv {max-frame-size}</code> command.	
Parameters	max-frame-size	Enter the keywords <code>max-frame-size</code> to advertise the dot3 maximum frame size.
Defaults	none	
Command Modes	CONFIGURATION (conf- <code>lldp</code>) and INTERFACE (conf-if- <i>interface</i> - <code>lldp</code>)	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

Z9500

Syntax

```
advertise management-tlv {management-address | system-  
capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the `no advertise management-tlv {management-address | system-capabilities | system-description | system-name} command`.

Parameters

management-address	Enter the keyword <code>management-address</code> to advertise the management IP address TLVs to the LLDP peer.
system-capabilities	Enter the keywords <code>system-capabilities</code> to advertise the system capabilities TLVs to the LLDP peer.
system-description	Enter the keywords <code>system-description</code> to advertise the system description TLVs to the LLDP peer.
system-name	Enter the keywords <code>system-name</code> to advertise the system name TLVs to the LLDP peer.

Defaults

none

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Modified to support management-address parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The command options `management-address`, `system-capabilities`, `system-description`, and `system-name` can be invoked individually or together, in any sequence.

advertise management-tlv (Interface)

Advertise management type, length, values (TLVs) to the specified interface.

Z9500

Syntax `advertise management-tlv {management-address | system-capabilities | system-description | system-name}`
 To remove advertised management TLVs, use the `no advertise management-tlv {management-address | system-capabilities | system-description | system-name} command`.

Parameters

management-address	Enter the keywords <code>management-address</code> to advertise the management IP address TLVs to the specified interface.
system-capabilities	Enter the keywords <code>system-capabilities</code> to advertise the system capabilities TLVs to the specified interface.
system-description	Enter the keywords <code>system-description</code> to advertise the system description TLVs to the specified interface.
system-name	Enter the keywords <code>system-name</code> to advertise the system name TLVs to the specified interface.

Defaults none

Command Modes INTERFACE (*conf-interface-lldp*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000 and S4810.
8.3.19.0	Introduced on the S4820T.

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Z9500

Syntax	<code>clear lldp counters interface</code>	
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Fast Ethernet interface, enter the keyword <code>FastEthernet</code> then the slot/ port information. - For a 10-Gigabit Ethernet interface, enter the keyword <code>tenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interface.

Z9500

Syntax	<code>clear lldp neighbors {interface}</code>	
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword <code>FastEthernet</code> then the slot/ port information. • For a 10-Gigabit Ethernet interface, enter the keyword <code>tenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

debug lldp interface

To display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets, enable LLDP debugging.

Z9500

Syntax	<code>debug lldp interface {interface all}{events packet {brief detail} {tx rx both}}</code>
---------------	--

To disable debugging, use the `no debug lldp interface {interface | all}{events} {packet {brief | detail} {tx | rx | both}}` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/ port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.



NOTE: The `FastEthernet` option is not supported on the S-Series.

all

(OPTIONAL) Enter the keyword `all` to display information on all interfaces.

events

(OPTIONAL) Enter the keyword `events` to display major events such as timer events.

packet

(OPTIONAL) Enter the keyword `packet` to display information regarding packets coming in or going out.

brief

(OPTIONAL) Enter the keyword `brief` to display brief packet information.

detail

(OPTIONAL) Enter the keyword `detail` to display detailed packet information.

tx

(OPTIONAL) Enter the keyword `tx` to display transmit-only packet information.

rx

(OPTIONAL) Enter the keyword `rx` to display receive-only packet information.

both

(OPTIONAL) Enter the keyword `both` to display both receive and transmit packet information.

Defaults

`none`

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version

Description

9.2(1.0)

Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

disable

Enable or disable LLDP.

Z9500

Syntax	<code>disable</code> To enable LLDP, use the <code>no disable</code> command.
Defaults	Enabled, that is no disable.
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if- <i>interface</i> -lldp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands	protocol lldp (Configuration) — enables LLDP globally. debug lldp interface — debugs LLDP. show lldp neighbors — displays the LLDP neighbors.
-------------------------	--

[show running-config lldp](#) — displays the LLDP running configuration.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

Z9500

Syntax	<code>hello seconds</code> To revert to the default, use the <code>no hello seconds</code> command.	
Parameters	seconds	Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is from 5 to 180 seconds. The default is 30 seconds .
Defaults	30 seconds	
Command Modes	CONFIGURATION (conf-lldp) and INTERFACE (conf-if- <i>interface</i> -lldp)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

management-interface

Enable and configure LLDP protocol parameters on the management interface.

Z9500

Syntax	<code>management-interface</code> To remove LLDP configuration on a management interface, use the <code>no management-interface</code> command.
--------	--

Command Modes	LLDP (conf-lddp)						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the Z9000 and S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2(0.0)	Introduced on the Z9000 and S4810.
Version	Description						
9.2(1.0)	Introduced on the Z9500.						
9.2(0.0)	Introduced on the Z9000 and S4810.						
Usage Information	To enable LLDP on the management interface, use the <code>no disable</code> command in LLDP-MANAGEMENT-INTERFACE mode (conf-lddp-mgmtIf).						

mode

To receive or transmit, set LLDP.

Z9500

Syntax	<pre>mode {tx rx}</pre> To return to the default, use the <code>no mode {tx rx}</code> command.														
Parameters	<table> <tr> <td>tx</td><td>Enter the keyword <code>tx</code> to set the mode to transmit.</td></tr> <tr> <td>rx</td><td>Enter the keyword <code>rx</code> to set the mode to receive.</td></tr> </table>	tx	Enter the keyword <code>tx</code> to set the mode to transmit.	rx	Enter the keyword <code>rx</code> to set the mode to receive.										
tx	Enter the keyword <code>tx</code> to set the mode to transmit.														
rx	Enter the keyword <code>rx</code> to set the mode to receive.														
Defaults	Both transmit and receive .														
Command Modes	CONFIGURATION (conf-lddp) and INTERFACE (conf-if- <i>interface</i> -lddp)														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.7.1.0	Introduced on the S-Series.														
7.6.1.0	Introduced on the C-Series.														

Version	Description
7.4.1.0	Introduced on the E-Series.

Related Commands

[protocol lldp \(Configuration\)](#) — enables LLDP globally.

[show lldp neighbors](#) — displays the LLDP neighbors.

multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

Z9500

Syntax

`multiplier integer`

To return to the default, use the `no multiplier integer` command.

Parameters

integer

Enter the number of consecutive misses before the LLDP declares the interface dead. The range is from 2 to 10.

Defaults

4 x hello

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

protocol lldp (Configuration)

Enable the LLDP globally on the switch.

Z9500

Syntax	<code>protocol lldp</code> To disable LLDP globally on the chassis, use the <code>no protocol lldp</code> command.
Defaults	Enabled.
Command Modes	CONFIGURATION (conf-lldp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

protocol lldp (Interface)

Enter the LLDP protocol in INTERFACE mode.

Z9500

Syntax	<code>[no] protocol lldp</code> To return to the global LLDP configuration mode, use the <code>no protocol lldp</code> command from Interface mode.
Defaults	LLDP is not enabled on the interface.
Command Modes	INTERFACE (conf-if- <i>interface</i> -lldp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

**Usage
Information**

Before LLDP can be configured on an interface, it must be enabled globally from CONFIGURATION mode. This command places you in LLDP mode on the interface; it does not enable the protocol.

When you enter the `LLDP` protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

show lldp neighbors

Display LLDP neighbor information for all interfaces or a specified interface.

Z9500

Syntax

```
show lldp neighbors [interface] [detail]
```

Parameters

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

detail

(OPTIONAL) Enter the keyword `detail` to display all the TLV information, remote management IP addresses, timers, and LLDP tx and rx counters.

Defaults

none

**Command
Modes**

EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Modified output of detail parameter to display remote management IP addresses.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

Example

```
R1(conf-if-te-1/31)#do show lldp neighbors
Loc PortID Rem Host Name Rem Port Id Rem Chassis
Id
-----
Te 1/21 R2 TenGigabitEthernet 2/11 00:01:e8:06:95:3e
Te 1/31 R3 TenGigabitEthernet 1/11 00:01:e8:09:c2:4a
```

show lldp statistics

Display the LLDP statistical information.

Z9500

Syntax `show lldp statistics`

Defaults `none`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show lldp statistics
Total number of neighbors: 300
Last table change time   : Mon Oct 02 16:00:52 2006
Number of Table Inserts  : 1621
Number of Table Deletes  : 200
Number of Table Drops    : 0
Number of Table Age Outs : 400
Dell#
```

show management-interface

Display LLDP management interface configuration information.

Z9500

Syntax show management-interface

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000 and S4810.

show running-config lldp

Display the current global LLDP configuration.

Z9500

Syntax show running-config lldp

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S8420T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show running-config lldp
!
protocol lldp
  advertise dot1-tlv port-protocol-vlan-id port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-capabilities system-
description
  hello 15
  multiplier 3
  no disable
Dell#
```

LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

The Dell Networking OS LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands. The C-Series and S-Series support all commands.

The E-Series generally supports the commands. However, LLDP-MED commands are more useful on the C-Series and the S50V model of the S-Series, because they support Power over Ethernet (PoE) devices.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific TLVs (Type Length Value), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- LLDP-MED Endpoint Device — any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- LLDP-MED Network Connectivity Device — any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

Regarding connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory

- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

To advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services, configure the system.

Z9500

Syntax

advertise med guest-voice {vlan-id layer2_priority DSCP_value}
| {priority-tagged number}
To return to the default, use the no advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

vlan-id

layer2_priority

DSCP_value

priority-tagged number

Enter the VLAN ID. The range is from 1 to 4094.

Enter the Layer 2 priority. The range is from 0 to 7.

Enter the DSCP value. The range is from 0 to 63.

Enter the keywords priority-tagged followed the Layer 2 priority. The range is from 0 to 7.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version

Description

9.2(1.0)

8.3.19.0

8.3.11.1

8.3.7.0

7.7.1.0

7.6.1.0

Introduced on the Z9500.

Introduced on the S4820T.

Introduced on the Z9000.

Introduced on the S4810.

Introduced on the S-Series.

Introduced on the C-Series and E-Series.

Related Commands

[protocol lldp \(Configuration\)](#) — enables LLDP globally.

[debug lldp interface](#) — debugs LLDP.

[show lldp neighbors](#) — displays the LLDP neighbors.

[show running-config lldp](#) — displays the LLDP running configuration.

advertise med guest-voice-signaling

To advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data, configure the system.

Z9500

Syntax

```
advertise med guest-voice-signaling {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med guest-voice-signaling
{vlan-id layer2_priority DSCP_value} | {priority-tagged number}
command.
```

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is from 0 to 7.
DSCP_value	Enter the DSCP value. The range is from 0 to 63.
priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

[debug lldp interface](#) — debugs LLDP.

[show lldp neighbors](#) — displays the LLDP neighbors.

[show running-config lldp](#) — displays the LLDP running configuration.

advertise med location-identification

To advertise a location identifier, configure the system.

Z9500

Syntax

```
advertise med location-identification {coordinate-based value |
civic-based value | ecs-elin value}

To return to the default, use the no advertise med location-
identification {coordinate-based value | civic-based value |
ecs-elin value} command.
```

Parameters

coordinate-based value	Enter the keywords <code>coordinate-based</code> then the coordinated based location in hexadecimal value of 16 bytes.
civic-based value	Enter the keywords <code>civic-based</code> then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
ecs-elin value	Enter the keywords <code>ecs-elin</code> then the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is from 10 to 25 characters.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Usage Information

- ECS — Emergency call service such as defined by TIA or the national emergency numbering association (NENA)
- ELIN — Emergency location identification number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

**Related
Commands**

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med power-via-mdi

To advertise the Extended Power via MDI TLV, configure the system.

Z9500

Syntax

`advertise med power-via-mdi`
To return to the default, use the `no advertise med power-via-mdi` command.

Defaults

unconfigured.

**Command
Modes**

CONFIGURATION (conf-lldp)

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.

**Usage
Information**

Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.

**Related
Commands**

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med softphone-voice

To advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone, configure the system.

Z9500

Syntax

```
advertise med softphone-voice {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med streaming-video

To advertise streaming video services for broadcast or multicast-based video, configure the system. This command does not include video applications that rely on TCP buffering.

Z9500

Syntax

```
advertise med streaming-video {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med streaming-video {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

Z9500

Syntax

```
advertise med video-conferencing {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med video-signaling

To advertise video control packets that use a separate network policy than video data, configure the system.

Z9500

Syntax

```
advertise med video-signaling {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

Z9500

Syntax `advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`
To return to the default, use the `no advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands [debug lldp interface](#) — debugs LLDP.
[show lldp neighbors](#) — displays the LLDP neighbors.
[show running-config lldp](#) — displays the LLDP running configuration.

advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

Z9500

Syntax

```
advertise med voice-signaling {vlan-id layer2_priority
DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters	vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
	layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged number	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

Microsoft Network Load Balancing

Network Load Balancing (NLB) is a clustering functionality that is implemented by Microsoft on Windows 2000 Server and Windows Server 2003 operating systems. Microsoft NLB clustering allows multiple servers running Microsoft Windows to be represented by one MAC and one IP address to provide transparent failover and load-balancing. The Dell Networking OS does not recognize server clusters by default; you must configure NLB functionality on a switch to support server clusters.

arp (for Multicast MAC Address)

To associate an IP address of a server cluster with a multicast MAC address in the switch for the multicast mode of network load balancing (NLB), use the address resolution protocol (ARP).

Syntax

```
arp ip-address multicast-mac-address interface
```

To remove an ARP address, use the `no arp ip-address` command.

Parameters

ip-address

Enter an IP address in dotted decimal format.

multicast-mac-address

Enter a 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic.

interface

Enter any of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- The specified interface must be configured using the `{output-range | output} interface` option with the `mac-address-table static` command.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for the association of an IP address with a multicast MAC address on the Z95000.
9.3(0.0)	Added support for the association of an IP address with a multicast MAC address on the S4810, S4820T, S6000, and Z9000.

Usage Information

For the multicast mode of NLB, use ARP to associate the IP address of a server cluster with a multicast MAC address in the switch, by entering the `arp ip-address multicast-mac-address` command.

Related Commands

[clear arp-cache](#) — clears dynamic ARP entries from the ARP table.

[show arp](#) — displays the ARP table.

ip vlan-flooding

Enable unicast data-traffic flooding on VLAN member ports.

Syntax

`ip vlan-flooding`

To disable, use the `no ip vlan-flooding` command.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Default

Disabled

Usage Information

By default this command is disabled. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.

mac-address-table static (for Multicast MAC Address)

To configure the multicast mode of network load balancing (NLB) on the switch, you must associate a multicast MAC address with the VLAN used to switch Layer 2 multicast traffic, and add output ports that will receive multicast streams on the VLAN in the MAC address table.

Syntax `mac-address-table static multicast-mac-address vlan vlan-id output-range {single-interface | interface-list | interface-range}`

To remove a MAC address, use the `no mac-address-table static multicast-mac-address vlan vlan-id output-range interface` command.

Parameters

- multicast-mac-address**

Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
- vlan vlan-id**

Enter a VLAN ID used to forward L2 multicast MAC traffic to a server cluster. Valid VLAN IDs are from 1 to 4094.
-  **NOTE:** Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.
- output-range interface**

For a multicast MAC address, enter the keyword `output-range` then one of the following interfaces for which traffic is forwarded:
 - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
 - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
 - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.3(0.0)	Added support for multicast MAC address on the MXL platform.

Usage Information When a multicast source and multicast receivers are in the same VLAN, you can configure a router so that multicast traffic is switched only to the ports assigned to a VLAN that is associated with a static multicast MAC address. However, before you

can configure a static MAC address and associate it with a VLAN used to switch Layer 2 multicast traffic, you must first enable the router for Layer 2 multicast switching with the `ip multicast-mode 12` command.

**Example
(Multicast)**

```
mac-address-table static 01:00:5E:01:00:01 vlan 2 output-range  
Te 0/2,Te 0/3
```

Multicast

The multicast commands are supported by Dell Networking operating system.
This chapter contains the following sections:

- [IPv4 Multicast Commands](#)
- [IPv6 Multicast Commands](#)

IPv4 Multicast Commands

This section describes the IPv4 multicast commands.

clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

Z9500

Syntax	<code>clear ip mroute {group-address [source-address] * snooping}</code>							
Parameters	group-address	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.						
	[source-address]							
	*	Enter * to clear all multicast routes.						
	snooping	Enter the keyword <code>snooping</code> to delete multicast snooping route table entries.						
Command Modes	EXEC Privilege							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2.(0.0)</td><td>Added support for keyword <code>snooping</code> on the Z9000, S4810, and S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2.(0.0)	Added support for keyword <code>snooping</code> on the Z9000, S4810, and S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
9.2.(0.0)	Added support for keyword <code>snooping</code> on the Z9000, S4810, and S4820T.							

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series.

Related Commands [show ip pim tib](#) — shows the PIM tree information base.

ip mroute

Assign a static mroute.

Z9500

Syntax

```
ip mroute destination mask {ip-address | null 0| {{bgp| ospf}
process-id | isis | rip | static} {ip-address | tag | null 0}}
[distance]
```

To delete a specific static mroute, use the `ip mroute destination mask {ip-address | null 0| {{bgp| ospf} process-id | isis | rip | static} {ip-address | tag | null 0}} [distance]` command.

To delete all mroutes matching a certain mroute, use the `no ip mroute destination mask` command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) or in dotted decimal format.
null 0	(OPTIONAL) Enter the keyword <code>null</code> then zero (0).
[protocol [process-id tag] ip-address]	(OPTIONAL) Enter one of the routing protocols: • Enter the BGP as-number then the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is from 1 to 65535. • Enter the OSPF process identification number then the IP address in dotted decimal format of the RPF neighbor. the range is from 1 to 65535. • Enter the IS-IS alphanumeric tag string then the IP address in dotted decimal format of the RPF neighbor. • Enter the RIP IP address in dotted decimal format of the RPF neighbor.
static ip-address	(OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
ip-address	(OPTIONAL) Enter the IP address in dotted decimal format of the RPF neighbor.

	<i>distance</i>	(OPTIONAL) Enter a number as the distance metric assigned to the mroute. The range is from 0 to 255.								
Defaults	Not configured.									
Command Modes	CONFIGURATION									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.3.19.0	Introduced on the S4820T.									
8.3.7.0	Introduced on the S4810.									
Related Commands	show ip mroute — views the E-Series routing table.									

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Z9500

Syntax	<code>ip multicast-limit <i>limit</i></code>											
Parameters	<i>limit</i>	Enter the desired maximum number of multicast entries on the system. The S-Series range is from 1 to 2000.										
Defaults	The S-Series default is 400 .											
Command Modes	CONFIGURATION											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the C-Series.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.19.0	Introduced on the S4820T.											
8.3.7.0	Introduced on the S4810.											
7.8.1.0	Introduced on the C-Series.											

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.6.1.0	Introduced on the E-Series.
Version	Description				
7.6.1.0	Introduced on the E-Series.				
Usage Information	This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile. To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the <code>ip multicast-limit</code> command is reached.				
Related Commands	show ip igmp groups — shows the IGMP groups.				

ip multicast-routing

Enable IP multicast forwarding.

Z9500

Syntax	<pre>ip multicast-routing</pre> To disable multicast forwarding, use the <code>no ip multicast-routing</code> command.										
Defaults	Disabled.										
Command Modes	CONFIGURATION										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.1</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.1	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.1	Introduced on the S4810.										
Usage Information	After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the <code>ip pim sparse-mode</code> command to enable IGMP and PIM on the interface.										

show ip mroute

View the multicast routing table.

Z9500

Syntax

```
show ip mroute [static | group-address [source-address] | count
| snooping [vlan vlan-id] [group-address [source-address]] |
summary | vlt [group-address [source-address] | count]
```

Parameters

static	(OPTIONAL) Enter the keyword <code>static</code> to view static multicast routes.
group-address [source-address]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
count	(OPTIONAL) Enter the keyword <code>count</code> to view the number of multicast routes and packets.
snooping [vlan vlan-id] [group-address [source-address]]	Enter the keyword <code>snooping</code> to display information on the multicast routes PIM-SM snooping discovers. Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094. Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a summary of all routes.
vlt	(OPTIONAL) Enter the keyword <code>vlt</code> to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword <code>count</code> to display the total number of multicast routes with the spanned IIF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Added support for keyword <code>vlt</code> to the Z9000, S4810, and S4820T.
8.4.1.1	Support for the keyword <code>snooping</code> and the optional <code>vlan</code> <code>vlan-id</code> , <code>group-address</code> , and <code>source-address</code> parameters were added on E-Series ExaScale.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example (Static)

```
Dell#show ip mroute static

Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change:
00:00:23
```

Example (Snooping)

```
Dell#show ip mroute snooping

IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13
    GigabitEthernet 4/20
```

Example (VLT)

```
Dell#show ip mroute vlt
IP Multicast Routing Table
Flags: S - Synced
```

```
(*, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
Spanned outgoing interface list:
  Vlan 20 (S)
  Vlan 30

(50.1.1.2, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
Spanned outgoing interface list:
  Vlan 20 (S)
```

Usage Information

The following describes the `show ip mroute` command shown in the following example.

Field	Description
(S, G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

Example

```
Dell#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: GigabitEthernet 3/4
  Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/4
```

show ip rpf

View reverse path forwarding.

Z9500

Syntax	show ip rpf
Command Modes	- EXEC - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage Information Network administrators use static mroutes to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reach-ability.



NOTE: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

```
Dell#show ip rpf
RPF information for 10.10.10.9
  RPF interface: Gi 3/4
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```

IPv6 Multicast Commands

This section describes the IPv6 multicast commands.

debug ipv6 mld_host

Enable the collection of debug information for MLD host transactions.

Z9500

Syntax [no] debug ipv6 mld_host [*int-count* | *interface type*] [slot/port-range]
To discontinue collection of debug information for the MLD host transactions, use the no debug ipv6 mld_host command.

Parameters

<i>int-count</i>	Enter the keyword count to indicate the number of required debug messages.
<i>interface type</i>	Enter the following keywords and slot/port information: - For a 10G Ethernet interface, enter the keyword tengigabitethernet then the slot/port information. - For a 40G interface, enter the keyword fortyGigE then the slot/port information. - For a management interface, enter the keyword managementinterface then the slot/port information. - For a port-channel interface, enter the keywords port-channel then the slot/port information. - For a VLAN interface, enter the keyword vlan then the slot/port information.

Default Disabled

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage Information To debug the MLD protocol for all ports or for specified ports, use the debug ipv6 mld_host command. Displayed information includes when a query is received, when a report is sent, when a mcast joins or leaves a group, and some reasons why an MLD query is rejected.

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Z9500

Syntax	ip multicast-limit limit													
Parameters	limit	Enter the desired maximum number of multicast entries on the system. The S-Series range is from 1 to 2000.												
Defaults	The S-Series default is 400 .													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the C-Series.	7.6.1.0	Introduced on the E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.7.0	Introduced on the S4810.													
7.8.1.0	Introduced on the C-Series.													
7.6.1.0	Introduced on the E-Series.													
Usage Information	This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile. To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the ip multicast-limit command is reached.													
Related Commands	show ip igmp groups — shows the IGMP groups.													

Multicast Source Discovery Protocol (MSDP)

Multicast source discovery protocol (MSDP) connects multiple PIM Sparse-Mode (PIM-SM) domains together.

MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

Z9500

Syntax	<code>clear ip msdp peer {peer address}</code>	
Parameters	peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
Defaults	Not configured.	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
6.2.1.1	Introduced

clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Z9500

Syntax `clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters	group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).
	rejected-sa	Enter the keywords <code>rejected-sa</code> to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
	local	Enter the keyword <code>local</code> to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults Without any options, this command clears the entire source-active cache.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the <code>local</code> option.
7.7.1.0	Added the <code>rejected-sa</code> option.
6.2.1.1	Introduced

clear ip msdp statistic

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Z9500

Syntax	clear ip msdp sa-cache [group-address rejected-sa local]		
Parameters	group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).	
	rejected-sa	Enter the keyword rejected-sa to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.	
	local	Enter the keyword local to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.	
Defaults	Without any options, this command clears the entire source-active cache.		
Command Modes	EXEC Privilege		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .		

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the <code>local</code> option.
7.7.1.0	Added the <code>rejected-sa</code> option.
6.2.1.1	Introduced

debug ip msdp

Turn on MSDP debugging.

Z9500

Syntax `debug ip msdp {event peer address | packet peer address | pim}`
To turn debugging off, use the `no debug ip msdp {event peer address | packet peer address | pim}` command.

Parameters	event <i>peer address</i>	Enter the keyword <code>event</code> then the peer address in a dotted decimal format (A.B.C.D.).
	packet <i>peer address</i>	Enter the keyword <code>packet</code> then the peer address in a dotted decimal format (A.B.C.D.).
	pim	Enter the keyword <code>pim</code> to debug advertisement from PIM.

Defaults Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

ip msdp cache-rejected-sa

Enable an MSDP cache for the rejected source-active entries.

Z9500

Syntax `ip msdp cache-rejected-sa {number}`
To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {number}` command then the `ip msdp cache-rejected-sa {number}` command.

Parameters	<i>number</i>	Enter the number of rejected SA entries to cache. The range is from 0 to 32766.												
Defaults	none													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.4.1.0</td><td>Introduced</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.4.1.0	Introduced
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.4.1.0	Introduced													
Related Commands	show ip msdp sa-cache rejected-sa													

ip msdp default-peer

Define a default peer from which to accept all source-active (SA) messages.

Z9500

Syntax	<pre>ip msdp default-peer <i>peer address</i> [<i>list name</i>]</pre> To remove the default peer, use the <code>no ip msdp default-peer {<i>peer address</i>} <i>list name</i></code> command.	
Parameters	<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.)
	<i>list name</i>	Enter the keywords <code>list name</code> and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.
Defaults	Not configured.	
Command Modes	CONFIGURATION	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added the <code>list</code> option and removed the <code>prefix-list</code> option.
7.4.1.0	Introduced

Usage Information

If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple `default peer` commands.

ip msdp log-adjacency-changes

Enable logging of MSDP adjacency changes.

Z9500

Syntax

`ip msdp log-adjacency-changes`

To disable logging, use the `no ip msdp log-adjacency-changes` command.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
6.2.1.1	Introduced

ip msdp mesh-group

To be a member of a mesh group, configure a peer.

Z9500

Syntax	<pre>ip msdp mesh-group {name} {peer address}</pre> To remove the peer from a mesh group, use the <code>no ip msdp mesh-group {name} {peer address}</code> command.													
Parameters	<i>name</i> Enter a string of up to 16 characters long for as the mesh group name. <i>peer address</i> Enter the peer address in a dotted decimal format (A.B.C.D.).													
Defaults	Not configured.													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>6.2.1.1</td><td>Introduced</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	6.2.1.1	Introduced
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
6.2.1.1	Introduced													
Usage Information	An MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain's MSDP speakers are fully meshed, they can be configured into a mesh-group. If member X of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member X accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member X cannot forward the SA message to other members of the mesh-group.													

ip msdp originator-id

Configure the MSDP Originator ID.

Z9500

Syntax	<pre>ip msdp originator-id {interface}</pre> To remove the originator-id, use the <code>no ip msdp originator-id {interface}</code> command.	
Parameters	interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
6.2.1.1	Introduced

ip msdp peer

Configure an MSDP peer.

Z9500

Syntax

```
ip msdp peer peer address [connect-source] [description] [sa-limit number]
```

To remove the MSDP peer, use the `no ip msdp peer peer address [connect-source interface] [description name] [sa-limit number]` command.

Parameters	<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.).
	<i>connect-source interface</i>	Enter the keywords <code>connect-source</code> then one of the interfaces and slot/port or number information: - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>description name</i>	(OPTIONAL) Enter the keyword <i>description</i> then a description name (maximum 80 characters) to designate a description for the MSDP peer.
	<i>sa-limit number</i>	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000. The default it 500000 .

Defaults As described in the *Parameters* section.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
	7.5.1.0	Added option for SA upper limit and the <code>description</code> option.
	6.2.1.1	Introduced
Usage Information	The <code>connect-source</code> option is used to supply a source IP address for the TCP connection. When an interface is specified using the <code>connect-source</code> option, the primary configured address on the interface is used. If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages continue to be accepted. To enforce the limit in such situation, use the <code>clear ip msdp peer</code> command to reset the peer.	
Related Commands	ip msdp sa-limit — configures the MSDP SA Limit. clear ip msdp peer — clears the MSDP peer. show ip msdp — displays the MSDP information.	

ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which the ACL denies time out and are not refreshed. Until they time out, they continue to reside in the MSDP SA cache.

Z9500

Syntax	<code>ip msdp redistribute [list <i>acl-name</i>]</code>	
Parameters	list <i>acl-name</i>	Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Introduced
Usage Information	Modifications to the ACL do not have an immediate effect on the sa-cache.	
	To apply the redistribute filter to entries already present in the SA cache, use the <code>clear ip msdp sa-cache local</code> command.	

ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

Z9500

Syntax	<code>ip msdp sa-filter {in out} peer-address list [access-list name]</code>	
	Remove this configuration using the <code>no ip msdp sa-filter {in out} peer address list [access-list name]</code> command.	
Parameters	in	Enter the keyword <code>in</code> to enable incoming SA filtering.
	out	Enter the keyword <code>out</code> to enable outgoing SA filtering.
	peer-address	Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
	access-list name	Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the E-Series.

ip msdp sa-limit

Configure the upper limit of source-active (SA) entries in SA-cache.

Z9500

Syntax	<code>ip msdp sa-limit <i>number</i></code> To return to the default, use the <code>no ip msdp sa-limit <i>number</i></code> command.													
Parameters	<i>number</i>	Enter the maximum number of SA entries in SA-cache. The range is from 0 to 40000.												
Defaults	50000													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.5.1.0	Introduced on the E-Series.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.5.1.0	Introduced on the E-Series.													
Usage Information	The system counts the SA messages originated by itself and those messages received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking). If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in the system continue to													

be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.

**Related
Commands**

[ip msdp peer](#) — configures the MSDP peer.

[clear ip msdp peer](#) — clears the MSDP peer.

[show ip msdp](#) — displays the MSDP information

ip msdp shutdown

Administratively shut down a configured MSDP peer.

Z9500

Syntax

```
ip msdp shutdown {peer address}
```

Parameters

peer address Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults

Not configured.

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

ip multicast-msdp

Enable MSDP.

Z9500

Syntax	<code>ip multicast-msdp</code> To exit MSDP, use the <code>no ip multicast-msdp</code> command.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

Z9500

Syntax	<code>show ip msdp {peer peer address sa-cache summary}</code>	
Parameters	peer peer address	Enter the keyword <code>peer</code> then the peer address in a dotted decimal format (A.B.C.D.).
	sa-cache	Enter the keywords <code>sa-cache</code> to display the Source-Active cache.
	summary	Enter the keyword <code>summary</code> to display an MSDP peer summary.
Defaults	Not configured.	

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

Example

```
Dell#show ip msdp peer 100.1.1.1

Peer Addr: 100.1.1.1
  Local Addr: 100.1.1.2(639) Connect Source: none
  State: Established Up/Down Time: 00:00:08
  Timers: KeepAlive 60 sec, Hold time 75 sec
  SourceActive packet count (in/out): 0/0
  SAs learned from this peer: 0
  SA Filtering:
    Input (S,G) filter: none
    Output (S,G) filter: none
Dell#
```

Example (Sa-cache)

```
Dell#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr  SourceAddr      RPAAddr      LearnedFrom Expire
UpTime
224.1.1.1  172.21.220.10  172.21.3.254  172.21.3.254 102
00:02:52
Dell#
```

Example (Summary)

```
Dell#show ip msdp summary
Peer Addr  Local Addr State      Source SA  Up/Down Description
72.30.1.2  72.30.1.1  Established none 0   00:00:03 peer1
72.30.2.2  72.30.2.1  Established none 0   00:00:03 peer2
72.30.3.2  72.30.3.1  Established none 0   00:00:02 test-peer-3
Dell#
```

show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

Z9500

Syntax `show ip msdp sa-cache rejected-sa`

Defaults `none`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.4.1.0	Introduced.

Example

```
Dell#show ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache 200 rejected SAs received, cache-size
1000
UpTime   GroupAddr SourceAddr RPAAddr   LearnedFrom Reason
00:00:13 225.1.2.1 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.2 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.3 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.4 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.5 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.6 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.7 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.8 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.9 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.10 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.12 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.13 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.14 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.15 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.16 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.17 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.18 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.19 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
Dell#
```

Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking operating system, conforms to IEEE 802.1s.

debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

Z9500

Syntax	<code>debug spanning-tree mstp [all bpdu interface {in out} events]</code>	
Parameters	all	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
	bpdu	(OPTIONAL) Enter the keyword <code>bpdu</code> to debug bridge protocol data units (BPDU).
	interface {in out}	(OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. Optionally, enter an <code>in</code> or <code>out</code> parameter with the optional interface: • For Receive, enter the keyword <code>in</code>. • For Transmit, enter the keyword <code>out</code>.
	events	(OPTIONAL) Enter the keyword <code>events</code> to debug MSTP events.
Command Modes	EXEC Privilege	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#debug spanning-tree mstp bpdu tengigabitethernet 2/0 ?  
in Receive (in)  
out Transmit (out)
```

disable

Globally disable the multiple spanning tree protocol on the switch.

Z9500

Syntax

`disable`

To enable MSTP, enter the `no disable` command.

Defaults

disabled.

Command Modes

MULTIPLE SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related Commands [protocol spanning-tree mstp](#) — enters MULTIPLE SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

Z9500

Syntax	<code>forward-delay seconds</code> To return to the default setting, use the <code>no forward-delay</code> command.	
Parameters	seconds	Enter the number of seconds the interface waits in the Blocking State and the Learning State before transiting to the Forwarding State. The range is from 4 to 30. The default is 15 seconds .
Defaults	15 seconds	
Command Modes	MULTIPLE SPANNING TREE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.5.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced.
Version	Description						
7.5.1.0	Introduced on the C-Series.						
6.5.1.0	Introduced.						
Related Commands	max-age — changes the wait time before MSTP refreshes protocol configuration information. hello-time — changes the time interval between bridge protocol data units (BPDUs).						

hello-time

Set the time interval between generation of MSTB bridge protocol data units (BPDUs).

Z9500

Syntax	<pre>hello-time seconds</pre> To return to the default value, use the <code>no hello-time</code> command.		
Parameters	<table> <tr> <td>seconds</td><td>Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is 2 seconds.</td></tr> </table>	seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is 2 seconds .
seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is 2 seconds .		
Defaults	2 seconds		
Command Modes	MULTIPLE SPANNING TREE		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.		

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related
Commands

[forward-delay](#) — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

[max-age](#) — changes the wait time before MSTP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the MSTB.

Z9500

Syntax

`max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

max-age

Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

Defaults

20 seconds

Command
Modes

MULTIPLE SPANNING TREE

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related
Commands

[forward-delay](#) — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

[hello-time](#) — changes the time interval between BPDUs.

max-hops

Configure the maximum hop count.

Z9500

Syntax	<code>max-hops number</code> To return to the default values, use the <code>no max-hops</code> command.	
Parameters	range	Enter a number for the maximum hop count. The range is from 1 to 40. The default is 20 .
Defaults	20 hops	
Command Modes	MULTIPLE SPANNING TREE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.1	Introduced on the S4810.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.5.1.0	Introduced.
Usage Information	The <code>max-hops</code> command is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reach zero, the switch discards the BPDU and ages out any information that it holds for the port.	

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

Z9500

Syntax `msti instance {vlan range | bridge-priority priority}`
To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

Parameters	msti instance	Enter the MSTP instance. The range is from zero (0) to 63.
	vlan range	Enter the keyword <code>vlan</code> then the identifier range value. The range is from 1 to 4094.
	bridge-priority priority	Enter the keywords <code>bridge-priority</code> then a value in increments of 4096 as the bridge priority. The range is from zero (0) to 61440. Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults default bridge-priority is **32768**.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information By default, all VLANs are mapped to MST instance zero (0) unless you use the `vlan range` command to map it to a non-zero instance.

name

The name you assign to the multiple spanning tree region.

Z9500

Syntax	<code>name region-name</code> To remove the region name, use the <code>no name</code> command.																
Parameters	region-name Enter the MST region name. The range is 32 character limit.																
Defaults	no default name.																
Command Modes	MULTIPLE SPANNING TREE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.5.1.0</td><td>Introduced.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.5.1.0	Introduced.																
Usage Information	For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).																
Related Commands	msti — maps the VLAN(s) to an MST instance. revision — assigns the revision number to the MST configuration.																

protocol spanning-tree mstp

To enable and configure the multiple spanning tree group, enter MULTIPLE SPANNING TREE mode.

Z9500

Syntax	<pre>protocol spanning-tree mstp</pre> To disable the multiple spanning tree group, use the <code>no protocol spanning-tree mstp</code> command.																
Defaults	Not configured.																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	MSTP is not enabled when you enter MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter the <code>no disable</code> command while in MULTIPLE SPANNING TREE mode. For more information about the multiple spanning tree protocol, refer to the <i>Dell Networking OS Configuration Guide</i>.																
Example	<pre>Dell(conf)#protocol spanning-tree mstp Dell(config-mstp)#no disable</pre>																
Related Commands	disable — disables multiple spanning tree.																

revision

The revision number for the multiple spanning tree configuration.

Z9500

Syntax	<code>revision range</code> To return to the default values, use the <code>no revision</code> command.																	
Parameters	range	Enter the revision number for the MST configuration. The range is from 0 to 65535. The default is 0 .																
Defaults	0																	
Command Modes	MULTIPLE SPANNING TREE																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced on the E-Series.																	
Usage Information	For two MSTP switches to be within the same MST region, the switches must share the same revision number.																	
Related Commands	msti — maps the VLAN(s) to an MST instance. name — assigns the region name to the MST region.																	

show config

View the current configuration for the mode. Only non-default values are shown.

Z9500

Syntax `show config`

Command Modes MULTIPLE SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

Example

```
Dell(conf-mstp)#show config
!
protocol spanning-tree mstp
  no disable
  name CustomerSvc
  revision 2
  MSTI 10 VLAN 101-105
  max-hops 5
Dell(conf-mstp)#
```

show spanning-tree mst configuration

View the multiple spanning tree configuration.

Z9500

Syntax `show spanning-tree mst configuration`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI VID
 10 101-105
Dell#
```

show spanning-tree msti

View the multiple spanning tree instance.

Z9500

Syntax

```
show spanning-tree msti [instance-number [brief]] [guard]
```

Parameters

<i>instance-number</i>	(Optional) Enter the multiple spanning tree instance number. The range is from 0 to 63.
<i>brief</i>	(Optional) Enter the keyword <i>brief</i> to view a synopsis of the MST instance.
<i>guard</i>	(Optional) Enter the keyword <i>guard</i> to display the type of guard enabled on an MSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Support for the optional keyword <code>guard</code> was added on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display the port error disable state (EDS) loopback BPDU inconsistency causes.

Usage Information

Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree msti 10
MSTI 10 VLANs mapped 101-105

Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max
hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occurred 3058087

Port 82 (TenGigabitEthernet 2/0) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (TenGigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
The port is not in the portfast mode

Port 89 (TenGigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
```

```
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode
```

Example (EDS and LBK)

The bold line shows the loopback BPDU inconsistency (LBK_INC).

```
Dell#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max
hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
```

Interface						Designated		
Name	PortID	Prio	Cost	Sts	Cost	Bridge ID	PortID	
Te 0/0	128.257	128	20000	EDS	0	32768 0001.e801.6aa8	128.257	

Interface									
Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge	Boundary
Te 0/0	ErrDis	128.257	128	20000	EDS	0	P2P	No	No

```
Dell#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max
hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occurred 00:00:15 ago
on Te 0/0
```

Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding

```
Port path cost 20000, Port priority 128, Port Identifier
128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

Usage Information

The following describes the show spanning-tree msti 5 guard command shown in the following example.

Field	Description
Interface Name	MSTP interface.

Field	Description
Instance	MSTP instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```
Dell#show spanning-tree msti 5 guard
Interface
Name      Instance  Sts Guard      type
-----
Te 0/1    5          INCON (Root)  Rootguard
Te 0/2    5          FWD           Loopguard
Te 0/3    5          EDS (Shut)    Bpduguard
```

spanning-tree

Enable the multiple spanning tree protocol on the interface.

Z9500

Syntax

`spanning-tree`

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

spanning-tree Enter the keywords `spanning-tree` to enable the MSTP on the interface.

Defaults

Enable.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

Z9500

Syntax	<code>spanning-tree msti <i>instance</i> {cost <i>cost</i> priority <i>priority</i>}</code>	
Parameters	msti <i>instance</i>	Enter the keyword <code>msti</code> and the MST instance number. The range is from zero (0) to 63.
	cost <i>cost</i>	(OPTIONAL) Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: 10-Gigabit Ethernet interface = 2000 - Port Channel interface with one 10 Gigabit Ethernet = 2000 - Port Channel with two 10 Gigabit Ethernet = 1800
	priority <i>priority</i>	Enter keyword <code>priority</code> then a value in increments of 16 as the priority. The range is from 0 to 240. The default is 128 .
Defaults	- cost = depends on the interface type - priority = 128	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

spanning-tree mstp edge-port

Configures the interface as an MST edge port and optionally a Bridge Protocol Data Unit (BPDU) guard.

Z9500

Syntax	<code>spanning-tree mstp edge-port [bpduguard [shutdown-on-violation]]</code>	
Parameters	mstp edge-port	Enter the keyword <code>mstp</code> then the keywords <code>edge-port</code> to configure the interface as a Multiple Spanning Tree edge port.
	bpduguard	(OPTIONAL) Enter the keyword <code>portfast</code> to enable Portfast to move the interface into forwarding mode immediately after the root fails. Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.
	shutdown-onviolation	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
8.2.1.0	Introduced the hardware <code>shutdown-on-violation</code> option.

	Version	Description
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.5.1.0	Introduced on the E-Series.
Usage Information	On an MSTP switch, a port configured as an edge port immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with spanning-tree portfast enabled. If you do not enable <code>shutdown-on-violation</code>, BPDUs are still sent to the RPM CPU.	

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Z9500

Syntax	<pre>tc-flush-standard</pre> To disable, use the <code>no tc-flush-standard</code> command.																
Defaults	Disabled.																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.5.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.5.1.0	Introduced																
Usage Information	By default, the system implements an optimized flush mechanism for MSTP. This mechanism helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a																

standards-based flush mechanism is needed, this `knob` command can be turned on to enable flushing MAC addresses after receiving every topology change notification.

Open Shortest Path First (OSPFv2 and OSPFv3)

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP), which means that it distributes routing information between routers in a single Autonomous System (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) are the same for OSPFv2 and OSPFv3. OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

This chapter is divided into two sections. There is no overlap between the two sets of commands. You cannot use an OSPFv2 command in the IPv6 OSPFv3 mode.

- [OSPFv2 Commands](#)
- [OSPFv3 Commands](#)

 **NOTE:** The Dell Networking OS version 7.8.1.0 introduces Multi-Process OSPF on IPv4 (OSPFv2) only. It is not supported on OSPFv3 (IPv6).

The CLI requires that you include the Process ID when entering ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

OSPFv2 Commands

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328. .

area default-cost

Set the metric for the summary default route the area border router (ABR) generates into the stub area. Use this command on the border routers at the edge of a stub area.

Z9500

Syntax `area area-id default-cost cost`
To return default values, use the `no area area-id default-cost` command.

Parameters	<i>area-id</i>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	<i>cost</i>	Specifies the stub area's advertised external route metric. The range is from zero (0) to 65535.

Defaults	<code>cost = 1</code> ; no areas are configured.																		
Command Modes	ROUTER OSPF																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
7.8.1.0	Added support for the Multi-Process OSPF.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.1.1.1	Introduced on the E-Series.																		
Usage Information	In the Dell Networking operating software, <code>cost</code> is defined as reference bandwidth/bandwidth.																		
Related Commands	area stub — creates a stub area.																		

area nssa

Specify an area as a not so stubby area (NSSA).

Z9500

Syntax	<pre>area area-id nssa [default-information-originate] [no- redistribution] [no-summary]</pre> To delete an NSSA, use the <code>no area area-id nssa</code> command.	
Parameters	area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	no-redistribution	(OPTIONAL) Specify that the <code>redistribute</code> command does not distribute routes into the NSSA. Only use this command in an NSSA area border router (ABR).
	default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.

	no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.																		
Defaults	Not configured.																			
Command Modes	ROUTER OSPF																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
7.8.1.0	Added support for the Multi-Process OSPF.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			

area range

Summarize routes matching an address/mask at an area border router (ABR).

Z9500

Syntax	<pre>area area-id range ip-address mask [not-advertise]</pre> To disable route summarization, use the <code>no area area-id range ip-address mask</code> command.	
Parameters	area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	ip-address	Specify an IP address in dotted decimal format.
	mask	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
	not-advertise	(OPTIONAL) Enter the keywords <code>not-advertise</code> to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults	Not configured.																		
Command Modes	ROUTER OSPF																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
7.8.1.0	Added support for the Multi-Process OSPF.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.1.1.1	Introduced on the E-Series.																		
Usage Information	Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.																		
Related Commands	area stub — creates a stub area. router ospf — enters ROUTER OSPF mode to configure an OSPF instance.																		

area stub

Configure a stub area, which is an area not connected to other areas.

Z9500

Syntax	<pre>area area-id stub [no-summary]</pre> To delete a stub area, use the <code>no area area-id stub</code> command.	
Parameters	area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	no-summary	(OPTIONAL) Enter the keywords <code>no-summary</code> to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.
Defaults	Disabled.	

Command Modes	ROUTER OSPF																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
7.8.1.0	Added support for the Multi-Process OSPF.																		
7.6.1.0	Introduced on the S-Series.																		
7.5.1.0	Introduced on the C-Series.																		
6.1.1.1	Introduced on the E-Series.																		
Usage Information	To configure all routers and access servers within a stub, use this command.																		
Related Commands	router ospf — enters ROUTER OSPF mode to configure an OSPF instance.																		

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

Z9500

Syntax	<pre>auto-cost [reference-bandwidth <i>ref-bw</i>]</pre> To return to the default bandwidth or to assign cost based on the interface type, use the <code>no auto-cost [reference-bandwidth]</code> command.
Parameters	<i>ref-bw</i> (OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is 100 megabits per second.
Defaults	100 megabits per second.
Command Modes	ROUTER OSPF
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

clear ip ospf

Clear all OSPF routing tables.

Z9500

Syntax	<code>clear ip ospf <i>process-id</i> [process]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
	process	(OPTIONAL) Enter the keyword <code>process</code> to reset the OSPF process.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

Z9500

Syntax	<code>clear ip ospf <i>process-id</i> statistics [interface <i>name</i> {neighbor <i>router-id</i>}]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
	<i>interface name</i>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: • For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	<i>neighbor router-id</i>	(OPTIONAL) Enter the keyword <code>neighbor</code> then the neighbor's router-id in dotted decimal format (A.B.C.D.).
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related
Commands

[show ip ospf statistics](#) — displays the OSPF statistics.

debug ip ospf

Display debug information on OSPF. Entering the `debug ip ospf` commands enables OSPF debugging for the first OSPF process.

Z9500

Syntax

```
debug ip ospf process-id [bfd |event | packet | spf | database-  
timer rate-limit]
```

To cancel the debug command, use the `no debug ip ospf` command.

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
bfd	(OPTIONAL) Enter the keyword <code>bfd</code> to debug only OSPF BFD information.
event	(OPTIONAL) Enter the keyword <code>event</code> to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword <code>packet</code> to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword <code>spf</code> to display the Shortest Path First information.
database-timer rate-limit	(OPTIONAL) Enter the keywords <code>database-timer rate-limit</code> to display the LSA throttling timer information. This applies to the S4810 platform only.

Command
Modes

EXEC Privilege

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the <code>database-timer rate-limit</code> option for the S4810.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `debug ip ospf` command shown in the Example below.

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.
v:	Displays the OSPF version. The system supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the <code>ip ospf authentication-key</code> command • 2 - MD5 authentication configured using the <code>ip ospf message-digest-key</code> command
auk:	If the <code>ip ospf authentication-key</code> command is configured, this field displays the key used.
keyid:	If the <code>ip ospf message-digest-key</code> command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority

Field	Description
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)
hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

Example

```

Dell#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

Dell#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) 1:44 rid:192.1.1.1
      aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Te 1/3 dst:
224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0

```

default-information originate

To generate a default external route into an OSPF routing domain, configure the system.

Z9500

Syntax

```

default-information originate [always] [metric metric-value]
[metric-type type-value] [route-map map-name]

```

To return to the default values, use the `no default-information originate` command.

Parameters

always (OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.

	metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to configure a metric value for the route. The range is from 1 to 16777214.																		
	metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> then an OSPF link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route																		
	route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of an established route map.																		
Defaults	Disabled.																			
Command Modes	ROUTER OSPF																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
7.8.1.0	Added support for the Multi-Process OSPF.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			
Related Commands	redistribute — redistributes routes from other routing protocols into OSPF.																			

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the `redistribute` command.

Z9500

Syntax	<pre>default-metric <i>number</i></pre> To return to the default values, use the <code>no default-metric [number]</code> command.
---------------	--

Parameters	<i>number</i>	Enter a number as the metric. The range is from 1 to 16777214.																		
Defaults	Disabled.																			
Command Modes	ROUTER OSPF																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
7.8.1.0	Added support for the Multi-Process OSPF.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			
Related Commands	redistribute — redistributes routes from other routing protocols into OSPF.																			

description

Add a description about the selected OSPF configuration.

Z9500

Syntax	<code>description <i>description</i></code> To remove the OSPF description, use the <code>no description</code> command.
Parameters	<i>description</i> Enter a text string description to identify the OSPF configuration (80 characters maximum).
Defaults	none
Command Modes	ROUTER OSPF
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands [show ip ospf asbr](#) — displays the VLAN configuration.

distance

Define an administrative distance for particular routes to a specific IP address.

Z9500

Syntax `distance weight [ip-address mask access-list-name]`
 To delete the settings, use the `no distance weight [ip-address mask access-list-name]` command.

Parameters	weight	Specify an administrative distance. The range is from 1 to 255. The default is 110 .
	ip-address	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, include the mask for that router address.
	mask	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
	access-list-name	(OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.

Defaults **110**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

distance ospf

Configure an OSPF distance metric for different types of routes.

Z9500

Syntax	<pre>distance ospf [external <i>dist3</i>] [inter-area <i>dist2</i>] [intra-area <i>dist1</i>]</pre> To delete these settings, use the <code>no distance ospf</code> command.	
Parameters	external <i>dist3</i> (OPTIONAL) Enter the keyword <code>external</code> then a number to specify a distance for external type 5 and 7 routes. The range is from 1 to 255. The default is 110. inter-area <i>dist2</i> (OPTIONAL) Enter the keywords <code>inter-area</code> then a number to specify a distance metric for routes between areas. The range is from 1 to 255. The default is 110. intra-area <i>dist1</i> (OPTIONAL) Enter the keywords <code>intra-area</code> then a number to specify a distance metric for all routes within an area. The range is from 1 to 255. The default is 110.	
Defaults	- external <i>dist3</i> = 110 - inter-area <i>dist2</i> = 110 - intra-area <i>dist1</i> = 110	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information To specify a distance for routes learned from other routing domains, use the `redistribute` command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

Z9500

Syntax `distribute-list prefix-list-name in [interface]`
 To delete a filter, use the `no distribute-list prefix-list-name in [interface]` command.

Parameters

<i>prefix-list-name</i>	Enter the name of a configured prefix list.
<i>interface</i>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: - For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

Z9500

Syntax

```
distribute-list prefix-list-name out [bgp | connected | isis |
rip | static]
```

To remove a filter, use the `no distribute-list prefix-list-name out [bgp | connected | isis | rip | static]` command.

Parameters

prefix-list-name

Enter the name of a configured prefix list.

bgp

(OPTIONAL) Enter the keyword `bgp` to specify that BGP routes are distributed.



NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.

connected

(OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.

isis

(OPTIONAL) Enter the keyword `isis` to specify that IS-IS routes are distributed.



NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.

rip

(OPTIONAL) Enter the keyword `rip` to specify that RIP routes are distributed.



NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.

	static	(OPTIONAL) Enter the keyword <code>static</code> to specify that only manually configured routes are distributed.																		
Defaults	Not configured.																			
Command Modes	ROUTER OSPF																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Added support for the Multi-Process OSPF.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Added support for the Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
7.8.1.0	Added support for the Multi-Process OSPF.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			
Usage Information	The <code>distribute-list out</code> command applies to routes autonomous system boundary routers (ASBRs) redistributes into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.																			

enable inverse-mask

By default, the system allows you to input the OSPF `network` command with a net-mask. This command provides a choice between inverse-mask or net-mask (the default).

Z9500

Syntax	<code>enable inverse mask</code> To return to the default net-mask, use the <code>no enable inverse mask</code> command.
Defaults	net-mask
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

fast-convergence

This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

Z9500

Syntax	<code>fast-convergence {number}</code> To cancel fast-convergence, use the <code>no fast convergence</code> command.	
Parameters	<i>number</i>	Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is from 1 to 4.
Defaults	none.	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on all platforms.

Usage Information	The higher this parameter is set, the faster OSPF converge takes place.	
		NOTE: The faster the convergence, the more frequent the route calculations and updates. This behavior impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking technical support.

flood-2328

Enable RFC-2328 flooding behavior.

Z9500

Syntax	<code>flood-2328</code> To disable, use the <code>no flood-2328</code> command.
Defaults	Disabled.
Command Modes	ROUTER OSPF
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information	In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC-2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links. By default, the system implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers. When you enable <code>flood-2328</code>, this command configures the system to flood LSAs on all interfaces.
--------------------------	--

graceful-restart grace-period

Specifies the time duration, in seconds, that the router's neighbors continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

Z9500

Syntax	<code>graceful-restart grace-period seconds</code>	
	To disable the grace period, use the <code>no graceful-restart grace-period</code> command.	
Parameters	seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is from 40 to 1800 seconds.
Defaults	Not Configured	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series. Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

Z9500

Syntax	<code>graceful-restart helper-reject ip-address</code>
	To return to default value, use the <code>no graceful-restart helper-reject</code> command.

Parameters	<i>ip-address</i>	Enter the OSPF router-id, in IP address format, of the restart router that <i>will not</i> act as a helper during graceful restart.
Defaults	Not configured.	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	<code>Restart role</code> enabled on the S-Series (Both <code>Helper</code> and <code>Restart</code> roles now supported on S-Series). Added support for Multi-Process OSPF.
7.7.1.0	Added <code>Helper-Role</code> support on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart mode

Enable the graceful restart mode.

Z9500

Syntax	<code>graceful-restart mode [planned-only unplanned-only]</code> To disable graceful restart mode, use the <code>no graceful-restart mode</code> command.	
Parameters	planned-only	(OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only.
	unplanned-only	(OPTIONAL) Enter the keywords <code>unplanned-only</code> to indicate graceful restart is supported in an unplanned restart condition only.
Defaults	Support for both planned and unplanned failures.	

Command Modes	ROUTER OSPF
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart role

Specify the role for your OSPF router during graceful restart.

Z9500

Syntax	<code>graceful-restart role [helper-only restart-only]</code> To disable graceful restart role, use the <code>no graceful-restart role</code> command.
---------------	---

Parameters	role helper-only	(OPTIONAL) Enter the keywords <code>helper-only</code> to specify the OSPF router is a helper only during graceful restart.
	role restart-only	(OPTIONAL) Enter the keywords <code>restart-only</code> to specify the OSPF router is a restart only during graceful-restart.

Defaults	By default, OSPF routers are both helper and restart routers during a graceful restart.
-----------------	---

Command Modes	ROUTER OSPF
----------------------	-------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF. Added <code>Restart</code> and <code>Helper</code> roles support on the S-Series.
7.7.1.0	Added <code>Helper-Role</code> support on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme until the grace period expires.

Z9500

Syntax `ip ospf auth-change-wait-time seconds`
To return to the default, use the `no ip ospf auth-change-wait-time` command.

Parameters `seconds` Enter the seconds. The range is from 0 to 300.

Defaults **zero (0) seconds.**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

Z9500

Syntax	<pre>ip ospf authentication-key [<i>encryption-type</i>] <i>key</i></pre> To delete an authentication key, use the <code>no ip ospf authentication-key</code> command.																	
Parameters	<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the key.																
	<i>key</i>	Enter an eight-character string. Strings longer than eight characters are truncated.																
Defaults	Not configured.																	
Command Modes	INTERFACE																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.1	Introduced on the E-Series.																	
Usage Information	All neighboring routers in the same network must use the same password to exchange OSPF information.																	

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

Z9500

Syntax	<pre>ip ospf cost cost</pre> To return to default value, use the <code>no ip ospf cost</code> command.
--------	---

Parameters	cost Enter a number as the cost. The range is from 1 to 65535.																
Defaults	The default cost is based on the reference bandwidth.																
Command Modes	INTERFACE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.1.1.1	Introduced on the E-Series.																
Usage Information	If this command is not configured, cost is based on the <code>auto-cost</code> command. When you configure OSPF over multiple vendors, to ensure that all routers use the same cost, use the <code>ip ospf cost</code> command. Otherwise, OSPF routes improperly.																
Related Commands	auto-cost — controls how the OSPF interface cost is calculated.																

ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

Z9500

Syntax	<pre>ip ospf dead-interval seconds</pre> To return to the default values, use the <code>no ip ospf dead-interval</code> command.
Parameters	seconds Enter the number of seconds for the interval. The range is from 1 to 65535. The default is 40 seconds.
Defaults	40 seconds

Command Modes	INTERFACE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.1.1.1	Introduced on the E-Series.																
Usage Information	By default, the dead interval is four times the default hello-interval.																
Related Commands	ip ospf hello-interval — sets the time interval between the hello packets.																

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Z9500

Syntax	<pre>ip ospf hello-interval seconds</pre> To return to the default value, use the <code>no ip ospf hello-interval</code> command.	
Parameters	seconds	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is 10 seconds .
Defaults	10 seconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information	The time interval between the hello packets must be the same for routers in a network.
Related Commands	ip ospf dead-interval — sets the time interval before a router is declared dead.

ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

Z9500

Syntax	<pre>ip ospf message-digest-key <i>keyid</i> md5 <i>key</i></pre> To delete a key, use the <code>no ip ospf message-digest-key <i>keyid</i></code> command.	
Parameters	<i>keyid</i>	Enter a number as the key ID. The range is from 1 to 255.
	<i>key</i>	Enter a continuous character string as the password.
Defaults	No MD5 authentication is configured.	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
9.1(0.0)	Included usage information on maximum number of digest keys per interface.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. The system sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell recommends keeping only one key per interface.



NOTE: The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

Z9500

Syntax

`ip ospf mtu-ignore`

To return to the default, use the `no ip ospf mtu-ignore` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf network

Set the network type for the interface.

Z9500

Syntax	<code>ip ospf network {broadcast point-to-point}</code> To return to the default, use the <code>no ip ospf network</code> command.	
Parameters	broadcast	Enter the keyword <code>broadcast</code> to designate the interface as part of a broadcast network.
	point-to-point	Enter the keywords <code>point-to-point</code> to designate the interface as part of a point-to-point network.
Defaults	Not configured.	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

Z9500

Syntax	<code>ip ospf priority <i>number</i></code> To return to the default setting, use the <code>no ip ospf priority</code> command.																	
Parameters	<i>number</i>	Enter a number as the priority. The range is from 0 to 255. The default is 1 .																
Defaults	1																	
Command Modes	INTERFACE																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.1	Introduced on the E-Series.																	
Usage Information	Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router. Use this command for interfaces connected to multi-access networks, not point-to-point networks.																	

ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

Z9500

Syntax	<code>ip ospf retransmit-interval seconds</code>
--------	--

To return to the default values, use the `no ip ospf retransmit-interval` command.

Parameters

seconds

Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **5 seconds**.

This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults

5 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval must be larger for interfaces connected to virtual links.

ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

Z9500

Syntax

`ip ospf transmit-delay seconds`

To return to the default value, use the `no ip ospf transmit-delay` command.

Parameters

seconds

Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **1 second**.

This value must be greater than the transmission and propagation delays for the interface.

Defaults **1 second**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set the system.

Z9500

Syntax `log-adjacency-changes`
To disable the Syslog messages, use the `no log-adjacency-changes` command.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

maximum-paths

Enable the software to forward packets over multiple paths.

Z9500

Syntax	<code>maximum-paths number</code> To disable packet forwarding over multiple paths, use the <code>no maximum-paths</code> command.	
Parameters	number Specify the number of paths. The range for OSPFv2 is from 1 to 16. The default for OSPFv2 is 4 paths . The range for OSPFv3 is from 1 to 64. The default for OSPFv3 is 8 paths .	
Defaults	4	
Command Modes	ROUTER OSPF for OSPFv2 ROUTER OSPFv3 for OSPFv3	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

Z9500

Syntax	<code>mib-binding</code> To mib-binding on this OSPF process, use the <code>no mib-binding</code> command.												
Defaults	none.												
Command Modes	ROUTER OSPF												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced to all platforms.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced to all platforms.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
7.8.1.0	Introduced to all platforms.												
Usage Information	This command is either enabled or disabled. If no OSPF process is identified as the MIB manager, the first OSPF process is used. If an OSPF process has been selected, it must be disabled prior to assigning new process ID the MIB responsibility.												

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

Z9500

Syntax	<code>network ip-address mask area area-id</code> To disable an OSPF area, use the <code>no network ip-address mask area area-id</code> command.
---------------	--

Parameters

<i>ip-address</i>	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
<i>mask</i>	Enter a network mask in /prefix format. (/x)
<i>area-id</i>	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is from 0 to 65535. IP address format is dotted decimal format A.B.C.D.
	NOTE: If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced to all platforms.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To enable OSPF on an interface, the `network area` command must include, in its range of addresses, the primary IP address of an interface.

 **NOTE:** An interface can be attached only to a single OSPF area.

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

passive-interface

Suppress both receiving and sending routing updates on an interface.

Z9500

Syntax `passive-interface {default | interface}`

To enable both the receiving and sending routing, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

Parameters	default	Enter the keyword <code>default</code> to make all OSPF interfaces (current and future) passive.
	interface	Enter the following keywords and slot/port or number information: - For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Modified to include the keyword <code>default</code> .

	Version	Description
	6.1.1.1	Introduced on the E-Series.
Usage Information	Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent using other interfaces. The default keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the <code>no passive-interface interface</code> command. The <code>no</code> form of this command is inserted into the configuration for individual interfaces when the <code>no passive-interface interface</code> command is issued while <code>passive-interface default</code> is configured. This command behavior has changed as follows: <pre>passive-interface interface</pre> • The previous <code>no passive-interface interface</code> is removed from the running configuration. • The ABR status for the router is updated. • Save <code>passive-interface interface</code> into the running configuration. <pre>passive-interface default</pre> • All present and future OSPF interfaces are marked as <i>passive</i>. • Any adjacency is explicitly terminated from all OSPF interfaces. • All previous <code>passive-interface interface</code> commands are removed from the running configuration. • All previous <code>no passive-interface interface</code> commands are removed from the running configuration. <pre>no passive-interface interface</pre> • Remove the interface from the passive list. • The ABR status for the router is updated. • If <code>passive-interface default</code> is specified, then save <code>no passive-interface interface</code> into the running configuration. <pre>No passive-interface default</pre> • Clear everything and revert to the default behavior. • All previously marked passive interfaces are removed. • May update ABR status.	

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

Z9500

Syntax `redistribute {connected | rip | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]`
To disable redistribution, use the `no redistribute {connected | isis | rip | static}` command.

Parameters	connected	Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.
	rip	Enter the keyword <code>rip</code> to specify that RIP routing information is redistributed.
	static	Enter the keyword <code>static</code> to specify that information from static routes is redistributed.
	metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 16777214.
	metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: • 1 = OSPF External type 1 • 2 = OSPF External type 2
	route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
	tag <i>tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> then a number. The range is from 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

	Version	Description
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Added support for Multi-Process OSPF.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.1.1.1	Introduced on the E-Series.
Usage Information	To redistribute the default route (0.0.0.0/0), configure the <code>default-information originate</code> command.	
Related Commands	default-information originate — generates a default route into the OSPF routing domain.	

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

Z9500

Syntax	<pre>redistribute bgp as <i>number</i> [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [tag <i>tag-value</i>]</pre> To disable redistribution, use the <code>no redistribute bgp as <i>number</i> [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-name</i>] [tag <i>tag-value</i>]</code> command.	
Parameters	<i>as number</i>	Enter the autonomous system number. The range is from 1 to 65535.
	<i>metric metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then the metric-value number. The range is from 0 to 16777214.
	<i>metric-type type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: 1 = for OSPF External type 1 2 = for OSPF External type 2
	<i>route-map map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
	<i>tag tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.
Defaults	none	
Command Modes	ROUTER OSPF	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.3	Added Route Map for BGP Redistribution to OSPF.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the keyword <code>default</code> .
6.1.1.1	Introduced on the E-Series.

redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

Z9500

Syntax

```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric
metric-value | metric-type type-value] [route-map map-name]
[tag tag-value]
```

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value] command`.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords <code>level-1</code> to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords <code>level-1-2</code> to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords <code>level-2</code> to redistribute only IS-IS Level-2 routes.
metric metric-value	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 4294967295.

	metric-type type-value	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: 1 = for OSPF External type 1 2 = for OSPF External type 2
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
	tag tag-value	(OPTIONAL) Enter the keyword <code>tag</code> to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.
Defaults	Not configured.	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

router-id

To configure a fixed router ID, use this command.

Z9500

Syntax	<code>router-id ip-address</code> To remove the fixed router ID, use the <code>no router-id ip-address</code> command.	
Parameters	ip-address	Enter the router ID in the IP address format.
Defaults	none.	
Command Modes	ROUTER OSPF	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing the router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.

Example

```
Dell(conf)#router ospf 100
Dell(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:

Dell(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
Dell(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
Dell#
```

router ospf

To configure an OSPF instance, enter ROUTER OSPF mode.

Z9500

Syntax

```
router ospf process-id [vrf {vrf name}]
```

To clear an OSPF instance, use the `no router ospf process-id` command.

Parameters

process-id

Enter a number for the OSPF instance. The range is from 1 to 65535.

	vrf name (Optional) E-Series Only: Enter the VRF process identifier to tie the OSPF instance to the VRF. All network commands under this OSPF instance are then tied to the VRF instance.																						
Defaults	Not configured.																						
Command Modes	CONFIGURATION																						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Added support for OSPFv3 on the S4810 and Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.9.1.0</td><td>Added support for VRF.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for Multi-Process OSPF.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Added support for OSPFv3 on the S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.9.1.0	Added support for VRF.	7.8.1.0	Added support for Multi-Process OSPF.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																						
9.2(1.0)	Introduced on the Z9500.																						
9.1(0.0)	Added support for OSPFv3 on the S4810 and Z9000.																						
8.3.19.0	Introduced on the S4820T.																						
8.3.11.1	Introduced on the Z9000.																						
8.3.7.0	Introduced on the S4810.																						
7.9.1.0	Added support for VRF.																						
7.8.1.0	Added support for Multi-Process OSPF.																						
7.6.1.0	Introduced on the S-Series.																						
7.5.1.0	Introduced on the C-Series.																						
6.1.1.1	Introduced on the E-Series.																						
Usage Information	You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF. After the OSPF process and the VRF are tied together, you cannot use the OSPF Process ID again in the system.																						
Example	<pre>Dell(conf)#router ospf 2 Dell(conf-router_ospf)#</pre>																						

show config

Display the non-default values in the current OSPF configuration.

Z9500

Syntax	show config
Command Modes	ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell(config-router_ospf)#show config
!
router ospf 3
passive-interface FastEthernet 0/1
Dell(config-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

Z9500

Syntax

```
show ip ospf process-id [vrf vrf name]
```

Parameters

process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.8.0	Added output for LSA throttling timers.
8.3.7.0	Introduced on the S4810.
7.9.1.0	Added support for VRF.
7.8.1.0	Added support of Multi-Process OSPF.
7.8.1.0	Added the <i>process-id</i> option, in support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the `show ip ospf` command shown in the following example.

Line Beginning with	Description
"Routing Process..."	Displays the OSPF process ID and the IP address associated with the process ID.
"Supports only..."	Displays the number of Type of Service (TOS) routes supported.
"SPF schedule..."	Displays the delay and hold time configured for this process ID.
"Convergence Level"	
"Min LSA..."	Displays the intervals set for LSA transmission and acceptance.
"Number of..."	Displays the number and type of areas configured for this process ID.

Example

```
Dell#show ip ospf 10
Routing Process ospf 10 with ID 1.1.1.1 Virtual router default-
vrf
Supports only single TOS (TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
  Area BACKBONE (0)
    Number of interface in this area is 1
    SPF algorithm executed 205 times
    Area ranges are
Dell#
```

Related
Commands

[show ip ospf database](#) — displays information about the OSPF routes configured.

[show ip ospf interface](#) — displays the OSPF interfaces configured.

[show ip ospf neighbor](#) — displays the OSPF neighbors configured.

show ip ospf asbr

Display all autonomous system boundary router (ASBR) routers visible to OSPF.

Z9500

Syntax

```
show ip ospf process-id asbr
```

Parameters

process-id

Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults

none

Command
Modes

- EXEC
- EXEC Privilege

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support of Multi-Process OSPF.
7.8.1.0	Added the <i>process-id</i> option, in support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage
Information

To isolate problems with external routes, use this command. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.



NOTE: ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the following example, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-/).

Example

```
Dell#show ip ospf lasbr
```

RouterID	Flags	Cost	Nexthop	Interface	Area
3.3.3.3	-/-/-/	2	10.0.0.2	Te 0/1	1
1.1.1.1	E/-/-/	0	0.0.0.0	-	0

```
Dell#
```

show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

Z9500

Syntax

```
show ip ospf process-id database [database-summary]
```

Parameters

process-id

Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

database-summary

(OPTIONAL) Enter the keywords `database-summary` to the display the number of LSA types in each area and the total number of LSAs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database` command shown in the following example.

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

Example

```
Dell>show ip ospf 1 database

      OSPF Router with ID (11.1.2.1) (Process ID 1)
            Router (Area 0.0.0.0)
Link ID      ADV Router    Age   Seq#           Checksum Link count
11.1.2.1     11.1.2.1      673   0x80000005    0x707e   2
13.1.1.1     13.1.1.1      676   0x80000097    0x1035   2
192.68.135.2 192.68.135.2 1419  0x80000294    0x9cbd   1

            Network (Area 0.0.0.0)
Link ID      ADV Router    Age   Seq#           Checksum
10.2.3.2     13.1.1.1      676   0x80000003    0x6592
10.2.4.2     192.68.135.2 908   0x80000055    0x683e

            Type-5 AS External
Link ID      ADV Router    Age   Seq#           Checksum Tag
0.0.0.0      192.68.135.2 908   0x80000052    0xeb83   100
1.1.1.1      192.68.135.2 908   0x8000002a    0xbd27   0
10.1.1.0     11.1.2.1      718   0x80000002    0x9012   0
10.1.2.0     11.1.2.1      718   0x80000002    0x851c   0
10.2.2.0     11.1.2.1      718   0x80000002    0x7927   0
10.2.3.0     11.1.2.1      718   0x80000002    0x6e31   0
10.2.4.0     13.1.1.1      1184  0x80000068    0x45db   0
11.1.1.0     11.1.2.1      718   0x80000002    0x831e   0
11.1.2.0     11.1.2.1      718   0x80000002    0x7828   0
12.1.2.0     192.68.135.2 1663  0x80000054    0xd8d6   0
13.1.1.0     13.1.1.1      1192  0x8000006b    0x2718   0
13.1.2.0     13.1.1.1      1184  0x8000006b    0x1c22   0
172.16.1.0   13.1.1.1      148   0x8000006d    0x533b   0
Dell>
```

Related Commands

[show ip ospf database asbr-summary](#) — displays only ASBR summary LSA information.

show ip ospf database asbr-summary

Display information about autonomous system (AS) boundary LSAs.

Z9500

Syntax `show ip ospf process-id database asbr-summary [link-state-id]
[adv-router ip-address]`

Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
	<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the ip-address to display only the LSA information about that router.

- Command Modes**
- EXEC
 - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf database asbr-summary` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.

Example

```
Dell#show ip ospf 100 database asbr-summary

      OSPF Router with ID (1.1.1.10) (Process ID 100)

      Summary Asbr (Area 0.0.0.0)

LS age: 1437
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 103.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000000f
Checksum: 0x8221
Length: 28
Network Mask: /0
      TOS: 0 Metric: 2

LS age: 473
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 104.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000010
Checksum: 0x4198
```

Length: 28
--More--

Related Commands [show ip ospf database](#) — displays OSPF database information.

show ip ospf database external

Display information on the AS external (type 5) LSAs.

Z9500

Syntax `show ip ospf process-id database external [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database external` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
Metrics Type	Displays the external type.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.
Forward Address	Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.
External Route Tag	Displays the 32-bit field attached to each external route. The OSPF protocol does not use this field, but you can use the field for external route management.

Example

```
Dell#show ip ospf 1 database external

      OSPF Router with ID (20.20.20.5) (Process ID 1)
```

Type-5 AS External

```
LS age: 612
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 12.12.12.2
Advertising Router: 20.31.3.1
LS Seq Number: 0x80000007
Checksum: 0x4cde
Length: 36
Network Mask: /32
    Metrics Type: 2
    TOS: 0
    Metrics: 25
    Forward Address: 0.0.0.0
    External Route Tag: 43
```

```
LS age: 1868
Options: (No TOS-capability, DC)
LS type: Type-5 AS External
Link State ID: 24.216.12.0
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000005
Checksum: 0xa00e
Length: 36
Network Mask: /24
    Metrics Type: 2
    TOS: 0
    Metrics: 1
    Forward Address: 0.0.0.0
    External Route Tag: 701
Dell#
```

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database network

Display the network (type 2) LSA information.

Z9500

Syntax

```
show ip ospf process-id database network [link-state-id] [adv-  
router ip-address]
```

Parameters

process-id

Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

link-state-id

(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router ip-address (OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database network` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.

Field	Description
Checksum	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Example

```
Dell#show ip ospf 1 data network

      OSPF Router with ID (20.20.20.5) (Process ID 1)

          Network (Area 0.0.0.0)
      LS age: 1372
      Options: (No TOS-capability, DC, E)
      LS type: Network
      Link State ID: 202.10.10.2
      Advertising Router: 20.20.20.8
      LS Seq Number: 0x80000006
      Checksum: 0xa35
      Length: 36
      Network Mask: /24
          Attached Router: 20.20.20.8
          Attached Router: 20.20.20.9
          Attached Router: 20.20.20.7

          Network (Area 0.0.0.1)

      LS age: 252
      Options: (TOS-capability, No DC, E)
      LS type: Network
      Link State ID: 192.10.10.2
      Advertising Router: 192.10.10.2
      LS Seq Number: 0x80000007
      Checksum: 0x4309
      Length: 36
      Network Mask: /24
          Attached Router: 192.10.10.2
          Attached Router: 20.20.20.1
          Attached Router: 20.20.20.5
Dell#
```

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

Z9500

Syntax

```
show ip ospf database nssa-external [link-state-id] [adv-router
ip-address]
```

Parameters

link-state-id

(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router ip-address

(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

Z9500

Syntax

```
show ip ospf process-id database opaque-area [link-state-id]  
[adv-router ip-address]
```

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database opaque-area` command shown in the following example.

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item:

Item	Description
	• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

Example

```
Dell>show ip ospf 1 database opaque-area

      OSPF Router with ID (3.3.3.3) (Process ID 1)
      Type-10 Opaque Link Area (Area 0)

LS age: 1133
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.1
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000416
Checksum: 0x376
Length: 28
Opaque Type: 1
Opaque ID: 1
Unable to display opaque data

LS age: 833
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--
```

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database opaque-as

Display the opaque-as (type 11) LSA information.

Z9500

Syntax	<code>show ip ospf <i>process-id</i> database opaque-as [<i>link-state-id</i>] [<i>adv-router ip-address</i>]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
	<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the ip-address to display only the LSA information about that router.
Command Modes	- EXEC - EXEC Privilege	

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related
Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

Z9500

Syntax

```
show ip ospf process-id database opaque-link [link-state-id]
[adv-router ip-address]
```

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> then the IP address of an Advertising Router to display only the LSA information about that router.

Command
Modes

- EXEC
- EXEC Privilege

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

Related Commands [show ip ospf database](#) — displays OSPF database information.

show ip ospf database router

Display the router (type 1) LSA information.

Z9500

Syntax `show ip ospf process-id database router [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database router` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: - TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. - DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. - E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number detects duplicate or old LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Number of Links	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
Link connected to:	Identifies the type of network to which the router is connected.
(Link ID)	Identifies the link type and address.
(Link Data)	Identifies the router interface address.
Number of TOS Metric	Lists the number of TOS metrics.
TOS 0 Metric	Lists the number of TOS 0 metrics.

Example

```
Dell#show ip ospf 100 database router
      OSPF Router with ID (1.1.1.10) (Process ID 100)
```



```

Router (Area 0)

LS age: 967
Options: (No TOS-capability, No DC, E)
LS type: Router
Link State ID: 1.1.1.10
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000012f
Checksum: 0x3357
Length: 144
AS Boundary Router
Area Border Router
Number of Links: 10

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.68.129.1
(Link Data) Router Interface address: 192.68.129.1
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.68.130.1
(Link Data) Router Interface address: 192.68.130.1
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.68.142.2
(Link Data) Router Interface address: 192.68.142.2
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.68.141.2
(Link Data) Router Interface address: 192.68.141.2
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.68.140.2
(Link Data) Router Interface address: 192.68.140.2
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Stub Network
(Link ID) Network/subnet number: 11.1.5.0
--More--

```

Related Commands

[show ip ospf database](#) — displays OSPF database information.

show ip ospf database summary

Display the network summary (type 3) LSA routing information.

Z9500

Syntax

```
show ip ospf process-id database summary [link-state-id] [adv-
router ip-address]
```

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: - the network's IP address for Type 3 LSAs or Type 5 LSAs - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs - the default destination (0.0.0.0) for Type 5 LSAs
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id database summary` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item:

Item	Description
	• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the TOS options. Option 0 is the only option.
Metric	Displays the LSA metrics.

Example

```

Dell#show ip ospf 100 database summary

      OSPF Router with ID (1.1.1.10) (Process ID 100)

      Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
      TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
Network Mask: /24
      TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network

```

```

Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
TOS: 0 Metric: 1

```

**Related
Commands**

[show ip ospf database](#) — displays OSPF database information.

show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

Z9500

Syntax

```
show ip ospf process-id interface [interface]
```

Parameters

process-id

Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For the null interface, enter the keyword `null` then zero (0).
- For loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383.
- For tunnel interfaces, enter the keyword `tunnel` then a number from 0 to 16383.
- For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

**Command
Modes**

- EXEC
- EXEC Privilege

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id interface` command shown in the following example.

Item	Description
TenGigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time until the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

Example

```
Dell>show ip ospf int

TenGigabitEthernet 1/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
  BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address
```

```

192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface
address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.253.1 (Backup Designated
Router)

TenGigabitEthernet 1/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address
192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface
address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.253.5 (Designated Router)
  Adjacent with neighbor 192.168.253.3 (Backup Designated
Router)

Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type
LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host.
Dell>

```

show ip ospf neighbor

Display the OSPF neighbors connected to the local router.

Z9500

Syntax	<code>show ip ospf <i>process-id</i> neighbor</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf process-id neighbor` command shown in the following example.

Item	Description
Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until the system declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor's area (process ID).

Example

```
Dell#show ip ospf 34 neighbor
```

```
Neighbor ID Pri State      Dead Time Address  Interface Area
20.20.20.7  1 FULL/DR    00:00:32 182.10.10.3 Te 0/0 0.0.0.2
192.10.10.2 1 FULL/DR    00:00:37 192.10.10.2 Te 0/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER00:00:36 192.10.10.4 Te 0/1 0.0.0.1
Dell#
```

show ip ospf routes

Display routes OSPF calculates and stores in OSPF RIB.

Z9500

Syntax `show ip ospf process-id routes`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
-------------------	--

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

This command is useful in isolating routing problems between the OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

Example

```
Dell#show ip ospf 100 route
```

Prefix	Cost	Nexthop	Interface	Area	Type
1.1.1.1	1	0.0.0.0	Lo 0	0	Intra-Area
3.3.3.3	2	13.0.0.3	Te 0/47	1	Intra-Area
13.0.0.0	1	0.0.0.0	Te 0/47	0	Intra-Area
150.150.150.0	2	13.0.0.3	Te 0/47	-	External
172.30.1.0	2	13.0.0.3	Te 0/47	1	Intra-Area

```
Dell#
```

show ip ospf statistics

Display OSPF statistics.

Z9500

Syntax

```
show ip ospf process-id statistics global | [interface name  
{neighbor router-id}]
```


Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>global</i>	Enter the keyword <code>global</code> to display the packet counts received on all running OSPF interfaces and packet counts OSPF neighbors receive and transmit.
	<i>interface name</i>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: - For Port Channel groups, enter the keywords <code>port-channel</code> then a number. For the C-Series and S-Series, the range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>neighbor router-id</i>	(OPTIONAL) Enter the keyword <code>neighbor</code> then the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf statistics process-id global` command shown in the following example.

Row Heading	Description
Total	Displays the total number of packets the OSPF process receives/transmits.
Error	Displays the error count while receiving and transmitting packets by the OSPF process.
Hello	Number of OSPF Hello packets.
DDiscr	Number of database description packets.
LSReq	Number of link state request packets.
LSUpd	Number of link state update packets.
LSAck	Number of link state acknowledgement packets.
TxQ-Len	The transmission queue length.
RxQ-Len	The reception queue length.
Tx-Mark	The highest number mark in the transmission queue.
Rx-Mark	The highest number mark in the reception queue.
Hello-Q	The queue, for transmission or reception, for the hello packets.
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

The following describes the error definitions for the `show ip ospf statistics process-id global` command.

Error Type	Description
Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRP even though SELF is not a designated router.
Self-Org	Receive the self originated packet.
Wrong_Len	The received packet length is different to what was indicated in the OSPF header.
Invid-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.

Error Type	Description
Auth-Error	Simple authentication error.
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration.
No-Buffer	Buffer allocation failure.
Seq-no	A sequence no errors occurred during the database exchange process.
Socket	Socket Read/Write operation error.
Q-overflow	Packets dropped due to queue overflow.
Unknown-Pkt	Received packet is not an OSPF packet.

Example

```

Dell#show ip ospf 1 statistics global

OSPF Packet Count
  Total Error Hello DDiscr LSReq LSUpd LSAck
RX 10    0    8    2    0    0    0
TX 10    0   10    0    0    0    0

OSPF Global Queue Length
  TxQ-Len RxQ-Len Tx-Mark Rx-Mark
Hello-Q   0      0      0      2
LSR-Q     0      0      0      0
Other-Q   0      0      0      0

Error packets (Only for RX)

Intf-Down 0   Non-Dr    0   Self-Org 0
Wrong-Len 0   Invld-Nbr 0   Nbr-State 0
Auth-Err   0   MD5-Err   0   Chksum 0
Version    0   AreaMis   0   Conf-Issues 0
No-Buffer  0   Seq-No    0   Socket 0
Q-OverFlow 0   Unkown-Pkt 0

Error packets (Only for TX)

Socket Errors    0
Dell#

```

Usage Information

The `show ip ospf process-id statistics` command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
- The grace-timer remaining value for each interface
- The packet count received and transmitted for each neighbor

- Dead timer remaining value for each neighbor
- Transmit timer remaining value for each neighbor
- The LSU Q length and its highest mark for each neighbor
- The LSR Q length and its highest mark for each neighbor

Example (Statistics)

```
Dell#show ip ospf 100 statistics

Interface TenGigabitEthernet 0/8

    Hello-Timer 9, Wait-Timer 0, Grace-Timer 0
    Error packets (Only for RX)

Intf-Down 0 Non-Dr      0 Self-Orig  0
Wrong-Len 0 Invld-Nbr   0 Nbr-State 0
Auth-Error 0 MD5-Error  0 Cksum-Err 0
Version   0 AreaMisMatch 0 Conf-Issue 0
SeqNo-Err 0 Unkown-Pkt  0

Neighbor ID 9.1.1.2

    Hello DDiscr LSReq LSUpd LSAck
RX  59    3      1    1    1
TX  62    2      1    0    0

    Dead-Timer 37, Transmit-Timer 0
    LSU-Q-Len  0, LSU-Q-Wmark  0
    LSR-Q-Len  0, LSR-Q-Wmark  1
```

Related Commands

[clear ip ospf statistics](#) — clears the packet statistics in all interfaces and neighbors.

show ip ospf timers rate-limit

Show the LSA currently in the queue waiting for timers to expire.

Z9500

Syntax

```
show ip ospf process-id timers rate-limit
```

Parameters

process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ip ospf 10 timers rate-limit

List of LSAs in rate limit Queue
LSA id: 1.1.1.0 Type: 3 Adv Rtid: 3.3.3.3 Expiry time:
00:00:09.111
LSA id: 3.3.3.3 Type: 1 Adv Rtid: 3.3.3.3 Expiry time:
00:00:23.96
Dell#
```

show ip ospf topology

Display routers in directly connected areas.

Z9500

Syntax

```
show ip ospf process-id topology
```

Parameters

process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.

	Version	Description																		
	7.5.1.0	Introduced on the C-Series and E-Series.																		
Usage Information	To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.																			
Example	<pre>Dell#show ip ospf 1 topology</pre> <table><tr><th>Router ID</th><th>Flags</th><th>Cost</th><th>Nexthop</th><th>Interface</th><th>Area</th></tr><tr><td>3.3.3.3</td><td>E/B/-/</td><td>1</td><td>20.0.0.3</td><td>Te 13/1</td><td>0</td></tr><tr><td>1.1.1.1</td><td>E/-/-/</td><td>1</td><td>10.0.0.1</td><td>Te 7/1</td><td>1</td></tr></table> <pre>Dell#</pre>		Router ID	Flags	Cost	Nexthop	Interface	Area	3.3.3.3	E/B/-/	1	20.0.0.3	Te 13/1	0	1.1.1.1	E/-/-/	1	10.0.0.1	Te 7/1	1
Router ID	Flags	Cost	Nexthop	Interface	Area															
3.3.3.3	E/B/-/	1	20.0.0.3	Te 13/1	0															
1.1.1.1	E/-/-/	1	10.0.0.1	Te 7/1	1															

summary-address

To advertise one external route, set the OSPF ASBR.

Z9500

Syntax	<pre>summary-address ip-address mask [not-advertise] [tag tag-value]</pre> To disable summary address, use the <code>no summary-address ip-address mask</code> command.
---------------	--

Parameters	<i>ip-address</i>	Specify the IP address in dotted decimal format of the address to summarize.
	<i>mask</i>	Specify the mask in dotted decimal format of the address to summarize.
	<i>not-advertise</i>	(OPTIONAL) Enter the keywords <code>not-advertise</code> to suppress that match the network prefix/mask pair.
	<i>tag tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> then a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

Defaults	Not configured.
-----------------	-----------------

Command Modes	ROUTER OSPF
----------------------	-------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The `area range` command summarizes routes for the different areas.

With the `not-advertise` parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0, you can configure the `summary-address 1.1.0.0 255.255.0.0 not-advertise` to filter out all the routes fall in range 1.1.0.0/16.

Related Commands

[area range](#) — summarizes routes within an area.

timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

Z9500

Syntax

```
timers spf delay holdtime
```

To return to the default, use the `no timers spf` command.

Parameters

<i>delay</i>	Enter a number as the delay. The range is from 0 to 4294967295. The default is 5 seconds .
<i>holdtime</i>	Enter a number as the hold time. The range is from 0 to 4294967295. The default is 10 seconds .

Defaults

- delay = 5 seconds
- holdtime = 10 seconds

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information Setting the *delay* and *holdtime* parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.

timers throttle lsa all

Configure LSA transmit intervals.

Z9500

Syntax `timers throttle lsa all {start-interval | hold-interval | max-interval}`
 To return to the default, use the `no timers throttle lsa` command.

Parameters

start-interval	Set the minimum interval between initial sending and resending the same LSA. The range is from 0 to 600,000 milliseconds.
hold-interval	Set the next interval to send the same LSA. This interval is the time between sending the same LSA after the start-interval has been attempted. The range is from 1 to 600,000 milliseconds.
max-interval	Set the maximum amount of time the system waits before sending the LSA. The range is from 1 to 600,000 milliseconds.

Defaults

- start-interval: **0 msec**
- hold-interval: **5000 msec**
- max-interval: **5000 msec**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information LSAs are sent after the start-interval and then after hold-interval until the maximum interval is reached. In throttling, exponential backoff is used when sending same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the *start-interval 5000* and *hold-interval 1000* and *max-interval 100,000*, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, then 4000 until 100,000 msec is reached.

timers throttle lsa arrival

Configure the LSA acceptance intervals.

Z9500

Syntax `timers throttle lsa arrival arrival-time`
To return to the default, use the `no timers throttle lsa` command.

Parameters *arrival-time* Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is from 0 to 600,000 milliseconds.

Defaults **1000 msec**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

OSPFv3 Commands

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OFSPFv3 area.

Z9500

Syntax	<code>area <i>area-id</i> authentication ipsec spi <i>number</i> {MD5 SHA1} [key-encryption-type] key</code>	
Parameters	area <i>area-id</i>	Area for which OSPFv3 traffic is to be authenticated. For <i>area-id</i>, you can enter a number. The range is from 0 to 4294967295.
	ipsec spi <i>number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
	MD5 SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
	key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).
	key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).
Defaults	Not configured.	
Command Modes	ROUTER OSPFv3	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.4.2.0	Introduced on the E-Series TeraScale.

Usage Information

Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFv3 area with the `area encryption` command, you cannot use the `area authentication` command in the area at the same time.

The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

To remove an IPsec authentication policy from an OSPFv3 area, enter the `no area area-id authentication spi number` command.

Related Commands

[ipv6 ospf authentication](#) – configures an IPsec authentication policy on an OSPFv3 interface.

[show crypto ipsec policy](#) – displays the configuration of IPsec authentication policies.

area encryption

Configure an IPsec encryption policy for OSPFv3 packets in an OSPFv3 area.

Z9500

Syntax

```
area area-id encryption ipsec spi number esp encryption-  
algorithm [key-encryption-type] key authentication-algorithm  
[key-encryption-type] key
```

Parameters

area area-id

Area for which OSPFv3 traffic is to be encrypted. For *area-id*, enter a number.

The range is from 0 to 4294967295.

ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
esp encryption- algorithm	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
key- encryption- algorithm	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in encryption. The required lengths of a non-encrypted or encrypted key are: 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.
authentication- algorithm	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.
key- encryption- type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).
null	Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults

Not configured.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information

Before you enable IPsec encryption on an OSPFv3 interface, first enable OSPFv3 globally on the router. Configure the same encryption policy (same SPI and keys) on each interface in an OSPFv3 link.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router.

When you configure encryption for an OSPFv3 area with the `area encryption` command, you enable both IPsec encryption and authentication. However, when you enable authentication on an area with the `area authentication` command, you do not enable encryption at the same time.

If you have enabled IPsec authentication in an OSPFv3 area with the `area authentication` command, you cannot use the `area encryption` command in the area at the same time.

The configuration of IPsec encryption on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area encryption policy that has been configured is applied to the interface.

To remove an IPsec encryption policy from an interface, enter the `no area area-id encryption spi number` command.

Related Commands

[ipv6 ospf encryption](#) – configures an IPsec encryption policy on an OSPFv3 interface.

[show crypto ipsec policy](#) – display the configuration of IPsec encryption policies.

clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

Z9500

Syntax `clear ipv6 ospf process`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.

debug ipv6 ospf bfd

Display debug information and interface types for bidirectional forwarding detection (BFD) on OSPF IPv6 packets.

Z9500

Syntax `[no] debug ipv6 ospf bfd [interface]`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a tunnel interface, enter the keyword `tunnel` then a number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes	EXEC Privilege								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2.(0.0)</td><td>Introduced on the S4820T, S4810, and Z9000.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2.(0.0)	Introduced on the S4820T, S4810, and Z9000.		
Version	Description								
9.2(1.0)	Introduced on the Z9500.								
9.2.(0.0)	Introduced on the S4820T, S4810, and Z9000.								
Usage Information	The following section describes the command fields. <table> <tr> <th>Lines Beginning With or Including</th><th>Description</th></tr> <tr> <td>OSPFv3...</td><td>Debugging is on for all OSPFv3 packets and all interfaces.</td></tr> <tr> <td>05:21:01</td><td>Displays the time stamp.</td></tr> <tr> <td>Sending Ver:3</td><td>Sending OSPF3 version..</td></tr> </table>	Lines Beginning With or Including	Description	OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.	05:21:01	Displays the time stamp.	Sending Ver:3	Sending OSPF3 version..
Lines Beginning With or Including	Description								
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.								
05:21:01	Displays the time stamp.								
Sending Ver:3	Sending OSPF3 version..								
Example	<pre> Dell(conf-if-te-0/2)#do debug ipv6 ospf bfd te 0/2 OSPFv3 bfd related debugging is on for TenGigabitEthernet 0/2 00:59:26 : OSPFv3INFO: Received Interface mode bfd config command on interface Te 0/2 Enable 1, interval 0, min_rx 0, Multiplier 0, role 0, Disable 0 00:59:26 : OSPFv3INFO: Enabling BFD on interface Te 0/2 Cmd Add Session 00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP fe80:0000:0000:0000:0201:e8ff:fe8b:7720 00:59:27 : OSPFv3INFO: Completed Enabling BFD on interface Te 0/2 00:59:27 : OSPFv3INFO: Completed Interface mode BFD configuration on Te 0/2!! 00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP fe80:0000:0000:0000:0201:e8ff:fe8b:7720 00:59:27 : OSPFv3INFO: Ospf3_register_bfd ospf key 27648 00:59:27 : OSPFv3INFO: OSPFV3 Enabling BFD for NBRIP fe80:0000:0000:0000:0201:e8ff:fe8b:7720 Interface Te 0/2 IfIndex 34145282 00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3 role active 00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3 role active 00:59:27 : OSPFv3INFO: Completed Enabling BFD for NBRIP fe80:0000:0000:0000:0201:e8ff:fe8b:7720 Aug 25 11:19:59: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed session state to Init for neighbor fe80::201:e8ff:fe8b: 7720 on interface Te 0/2 (diag: NBR_DN) Aug 25 11:20:00: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed session state to Up for neighbor fe80::201:e8ff:fe8b: 7720 on interface Te 0/2 (diag: NO_DIAG) 00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg 00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Te 0/2 00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state </pre>								

debug ipv6 ospf packet

Display debug information and interface types on OSPF IPv6 packets.

Z9500

Syntax	debug ipv6 ospf {packet events} [<i>interface</i>]													
Parameters	<i>interface</i>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. The range is 1 to 128. • For a tunnel interface, enter the keyword <code>tunnel</code> then a number. The range is 1 to 16383. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.												
Command Modes	EXEC Privilege													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>7.8.1.0</td><td>Added support for C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced on the S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Added support for C-Series.	7.4.1.0	Introduced on E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.1.(0.0)	Introduced on the S4810 and Z9000.													
8.3.19.0	Introduced on the S4820T.													
7.8.1.0	Added support for C-Series.													
7.4.1.0	Introduced on E-Series.													
Example	<pre>Dell#debug ipv6 ospf packet OSPFv3 packet related debugging is on for all interfaces 05:21:01 : OSPFv3: Sending, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.254, Area ID:0, Inst:0, on Po 255 05:21:03 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.255, Area ID:0, Chksum:a177, Inst:0, from V1 100 05:20:25 : OSPFv3: Sending, Ver:3, Type:4(LS Update), Len:580, Router ID:223.255.255.254, Area ID:0, Inst:0, on V1 1000 07:21:40 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.254, Area ID:0, Chksum:af8f, Inst:0,</pre>													

from Te 0/36
Dell#

Command Fields	Lines Beginning With or Including	Description
	OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
	05:21:01	Displays the time stamp.
	Sending Ver:3	Sending OSPF3 version..
	type:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement • 7 - external LSA • 8 - link-state advertisement (OSPFv3) • 9 - link local LSA (OSPFv2), Intra-Area-Prefix LSA (OSPFv3) • 11 - grace LSA (OSPFv3)
	Length:	Displays the packet length.
	Router ID:	Displays the OSPF3 router ID.
	Area ID:	Displays the Area ID.
	Chksum:	Displays the OSPF3 checksum.

default-information originate

Configure the system to generate a default external route into an OSPFv3 routing domain.

Z9500

Syntax

```
default-information originate [always] [metric metric-value]  
[metric-type type-value] [route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

Parameters		
	always	(OPTIONAL) Enter the keyword <code>always</code> to specify that default route information must always be advertised.
	metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to configure a metric value for the route. The range is from 1 to 16777214.

	metric-type type-value	(OPTIONAL) Enter the keywords <code>metric-type</code> then an OSPFv3 link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route												
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of an established route map.												
Defaults	Disabled.													
Command Modes	ROUTER OSPFv3													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>7.8.1.0</td><td>Added support for C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced on the S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Added support for C-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.1.(0.0)	Introduced on the S4810 and Z9000.													
8.3.19.0	Introduced on the S4820T.													
7.8.1.0	Added support for C-Series.													
7.4.1.0	Introduced on the E-Series.													
Related Commands	redistribute — redistributes routes from other routing protocols into OSPFv3.													

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router's neighbors continues to advertise the router as adjacent during a graceful restart.

Z9500

Syntax	<code>graceful-restart grace-period seconds</code> To disable OSPFv3 graceful restart, enter <code>no graceful-restart grace-period</code> .	
Parameters	seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPFv3 terminates the process. The range is from 40 to 1800 seconds.
Defaults	OSPFv3 graceful restart is disabled and functions in a helper-only role.	

Command Modes	ROUTER OSPFv3										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr> <tr> <td>8.4.2.2</td><td>Introduced on the E-Series TeraScale.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Introduced on the S4810 and Z9000.	8.4.2.2	Introduced on the E-Series TeraScale.	8.3.19.0	Introduced on the S4820T.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
9.1(0.0)	Introduced on the S4810 and Z9000.										
8.4.2.2	Introduced on the E-Series TeraScale.										
8.3.19.0	Introduced on the S4820T.										
Usage Information	By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA. To enable OSPFv3 graceful restart, enter the <code>ipv6 router ospf</code> command to enter OSPFv3 configuration mode and then configure a grace period using the <code>graceful-restart grace-period</code> command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link. When you enable the helper-reject role on an interface with the <code>ipv6 ospf graceful-restart helper-reject</code> command, you reconfigure OSPFv3 graceful restart to function in a "restarting-only" role. In a "restarting-only" role, OSPFv3 does not participate in the graceful restart of a neighbor.										

graceful-restart mode

Specify the type of events that trigger an OSPFv3 graceful restart.

Z9500

Syntax	<code>graceful-restart mode {planned-only unplanned-only}</code> To disable graceful restart mode, enter <code>no graceful-restart mode</code> .	
Parameters	planned-only	(OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only.
	unplanned-only	(OPTIONAL) Enter the keywords <code>unplanned-only</code> to indicate graceful restart is supported in an unplanned restart condition only.

Defaults	OSPFv3 graceful restart supports both planned and unplanned failures.										
Command Modes	ROUTER OSPFv3										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr> <tr> <td>8.4.2.2</td><td>Introduced on the E-Series TeraScale.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Introduced on the S4810 and Z9000.	8.4.2.2	Introduced on the E-Series TeraScale.	8.3.19.0	Introduced on the S4820T.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
9.1(0.0)	Introduced on the S4810 and Z9000.										
8.4.2.2	Introduced on the E-Series TeraScale.										
8.3.19.0	Introduced on the S4820T.										
Usage Information	OSPFv3 graceful restart supports planned-only and/or unplanned-only restarts. The default is support for both planned and unplanned restarts. - A planned restart occurs when you enter the <code>redundancy force-failover rpm</code> command to force the primary RPM to switch to the backup RPM. During a planned restart, OSPF sends out a Type-11 Grace LSA before the system switches over to the backup RPM. - An unplanned restart occurs when an unplanned event causes the active RPM to switch to the backup RPM, such as when an active process crashes, the active RPM is removed, or a power failure happens. During an unplanned restart, OSPF sends out a Grace LSA when the backup RPM comes online. By default, both planned and unplanned restarts trigger an OSPFv3 graceful restart. Selecting one or the other mode restricts OSPFv3 to the single selected mode.										

ipv6 ospf area

Enable IPv6 OSPF on an interface.

Z9500

Syntax	<pre>ipv6 ospf process id areaarea id</pre> To disable OSPFv6 routing for an interface, use the <code>no ipv6 ospf process-id area area-id</code> command.	
Parameters	<i>process-id</i> Enter the process identification number. <i>area area-id</i> Specify the OSPF area. The range is from 0 to 65535.	
Defaults	none	
Command Modes	INTERFACE	
Modes		

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.4.1.0	Introduced on the E-Series and C-Series.

ipv6 ospf authentication

Configure an IPsec authentication policy for OSPFv3 packets on an IPv6 interface.

Z9500

Syntax

```
ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1}
[key-encryption-type] key}
```

Parameters

null	Causes an authentication policy configured for the area to not be inherited on the interface.
ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
MD5 SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on S4810 and Z9000.
8.4.2.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information

Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec authentication policy from an interface, enter the `no ipv6 ospf authentication spi number` command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf authentication null` command.

Related Commands

[area authentication](#) – configures an IPsec authentication policy for an OSPFv3 area.

[show crypto ipsec policy](#) – displays the configuration of IPsec authentication policies.

[show crypto ipsec sa ipv6](#) – displays the security associations set up for OSPFv3 interfaces in authentication policies.

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

Z9500

Syntax

```
ipv6 ospf bfd all-neighbors [disable | [interval interval  
min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command in interface mode..

Parameters

disable

(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.

	interval <i>milliseconds</i> (OPTIONAL) Enter the keyword <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100.						
	min_rx <i>milliseconds</i> Enter the keywords <code>min_rx</code> to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 100. The default is 100.						
	multiplier value Enter the keyword <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.						
	role [active passive] Enter the role that the local system assumes: • <code>Active</code> — The active system initiates the BFD session. Both systems can be active for the same session. • <code>Passive</code> — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is Active.						
Defaults	See Parameters						
Command Modes	INTERFACE						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2.0.0</td><td>Introduced on the Z9000, S4820T, and S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.2.0.0	Introduced on the Z9000, S4820T, and S4810.
Version	Description						
9.2(1.0)	Introduced on the Z9500.						
9.2.0.0	Introduced on the Z9000, S4820T, and S4810.						
Usage Information	This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure <code>ipv6 ospf bfd</code> in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the <code>bfd all-neighbors</code> command. Using the <code>no</code> form of this command does not disable BFD if you configure BFD in CONFIGURATION mode. To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword <code>disable</code>.						

ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

Z9500

Syntax	<code>ipv6 ospf interface-cost</code>	
Parameters	<i>interface-cost</i>	Enter a unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.
Defaults	Default cost based on the bandwidth.	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information	In general, the path cost is calculated as: $10^8 / \text{bandwidth}$ Using this formula, the default path cost is calculated as: • 10-Gigabit Ethernet—Default cost is 1 • 40-Gigabit Ethernet — Default cost is 1
-------------------	---

ipv6 ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

Z9500

Syntax	<code>ipv6 ospf dead-interval seconds</code> To return to the default time interval, use the <code>no ipv6 ospf dead-interval</code> command.
--------	--

Parameters	<i>seconds</i>	Enter the time interval in seconds. The range is from 1 to 65535 seconds.												
Defaults	40 seconds (Ethernet).													
Command Modes	INTERFACE													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>7.8.1.0</td><td>Added support for C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced on the S4810 and Z9000.	7.8.1.0	Added support for C-Series.	7.4.1.0	Introduced on the E-Series.	8.3.19.0	Introduced on the S4820T.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.1.(0.0)	Introduced on the S4810 and Z9000.													
7.8.1.0	Added support for C-Series.													
7.4.1.0	Introduced on the E-Series.													
8.3.19.0	Introduced on the S4820T.													
Usage Information	By default, the dead interval is four times longer than the default hello-interval.													
Related Commands	ipv6 ospf hello-interval – specifies the time interval between hello packets.													

ipv6 ospf encryption

Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

Z9500

Syntax	<pre>ipv6 ospf encryption {null ipsec spi number esp encryption- algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key}</pre>	
Parameters	null	Causes an encryption policy configured for the area to not be inherited on the interface.
	ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
	esp encryption-algorithm	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).										
key	Text string used in authentication. The required lengths of a non-encrypted or encrypted key are: 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.										
authentication-algorithm	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.										
key-encryption-type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).										
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).										
Defaults	Not configured.										
Command Modes	INTERFACE										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr> <tr> <td>8.4.2.0</td><td>Introduced on the E-Series TeraScale.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Introduced on the S4810 and Z9000.	8.4.2.0	Introduced on the E-Series TeraScale.	8.3.19.0	Introduced on the S4820T.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
9.1(0.0)	Introduced on the S4810 and Z9000.										
8.4.2.0	Introduced on the E-Series TeraScale.										
8.3.19.0	Introduced on the S4820T.										
Usage Information	Before you enable IPsec encryption on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.										

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same encryption policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec encryption policy from an interface, enter the `no ipv6 ospf encryption spi number` command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf no ipv6 ospf encryption null` command.

Related Commands

[area encryption](#) – configures an IPsec encryption policy for an OSPFv3 area.

[show crypto ipsec policy](#) – displays the configuration of IPsec encryption policies.

[show crypto ipsec sa ipv6](#) – displays the security associations set up for OSPFv3 interfaces in encryption policies.

ipv6 ospf graceful-restart helper-reject

Configure an OSPFv3 interface to not act upon the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

Z9500

Syntax

```
ipv6 ospf graceful-restart helper-reject
```

To disable the helper-reject role, enter `no ipv6 ospf graceful-restart helper-reject`.

Defaults

The helper-reject role is not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.4.2.2	Introduced on E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information

By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

The graceful-restart role command is not supported in OSPFv3. When you enable the helper-reject role on an interface, you reconfigure an OSPFv3 router to function in a "restarting-only" role.

ipv6 ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Z9500

Syntax	<code>ipv6 ospf hello-interval seconds</code> To return to the default time interval, enter <code>no ipv6 ospf hello-interval</code> .													
Parameters	seconds	Enter the time interval in seconds as the time between hello packets. The range is from 1 to 65525 seconds.												
Defaults	10 seconds (Ethernet).													
Command Modes	INTERFACE													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>7.8.1.0</td><td>Added support for the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Introduced on the S4810 and Z9000.	7.8.1.0	Added support for the C-Series.	7.4.1.0	Introduced on the E-Series.	8.3.19.0	Introduced on the S4820T.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.1(0.0)	Introduced on the S4810 and Z9000.													
7.8.1.0	Added support for the C-Series.													
7.4.1.0	Introduced on the E-Series.													
8.3.19.0	Introduced on the S4820T.													
Usage Information	The time interval between hello packets must be the same for routers in a network.													
Related Commands	ipv6 ospf dead-interval – specifies the time interval between hello packets was received from a router.													

Parameters	<i>process-id</i>	Enter the process identification number. The range is from 1 to 65535.
------------	-------------------	--

Defaults	none
----------	------

Command Modes	CONFIGURATION
---------------	---------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

maximum-paths

Enable the software to forward packets over multiple paths.

Z9500

Syntax	<code>maximum-paths number</code> To disable packet forwarding over multiple paths, use the <code>no maximum-paths</code> command.
--------	---

Parameters	<i>number</i>	Specify the number of paths. The range is from 1 to 64. The default is 8 paths.
------------	---------------	--

Defaults	8
----------	---

Command Modes	ROUTER OSPF
---------------	-------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

passive-interface

Disable (suppress) sending routing updates on an interface.

Z9500

Syntax	<code>passive-interface interface</code> To enable sending routing updates on an interface, use the <code>no passive-interface interface</code> command.					
Parameters	interface	Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.				
Defaults	Enabled, that is sending of routing updates are enabled by default.					
Command Modes	ROUTER OSPF for OSPFv2 ROUTER OSPFv3 for OSPFv3					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					

Version	Description
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

By default, no interfaces are *passive*. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

redistribute

Redistribute into OSPFv3.

Z9500

Syntax

```
redistribute {bgp as number}{connected | static}[metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

<i>bgp as number</i>	Enter the keyword <code>bgp</code> then the autonomous system number. The range is from 1 to 65535.
<i>connected</i>	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
<i>static</i>	Enter the keyword <code>static</code> to redistribute manually configured routes.
<i>metric metric-value</i>	Enter the keyword <code>metric</code> then the metric value. The range is from 0 to 16777214. The default is 20 .

	metric-type type-value (OPTIONAL) Enter the keywords <code>metric-type</code> then the OSPFv3 link state type of 1 or 2 for default routes. The values are: • 1 for a type 1 external route • 2 for a type 2 external route The default is 2.												
	route-map map-name (OPTIONAL) Enter the keywords <code>route-map</code> then the name of an established route map. If the route map is not configured, the default is deny (to drop all routes).												
	tag tag-value (OPTIONAL) Enter the keyword <code>tag</code> to set the tag for routes redistributed into OSPFv3. The range is from 0 to 4294967295 The default is 0.												
Defaults	Not configured.												
Command Modes	ROUTER OSPF for OSPFv2 ROUTER OSPFv3 for OSPFv3												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1.(0.0)</td><td>Introduced support for OSPFv3 on the S4810 and Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Added support for the C-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.												
8.3.19.0	Introduced on the S4820T.												
7.8.1.0	Added support for the C-Series.												
7.4.1.0	Introduced on the E-Series.												
Usage Information	To redistribute the default route (x::x::x::x), use the <code>default-information originate</code> command.												
Related Commands	default-information originate – configures default external route into OSPFv3.												

router-id

Designate a fixed router ID.

Z9500

Syntax	router-id ip-address To return to the previous router ID, use the no router-id ip-address command.													
Parameters	ip-address	Enter the router ID in the dotted decimal format.												
Defaults	The router ID is selected automatically from the set of IPv4 addresses configured on a router.													
Command Modes	ROUTER OSPF for OSPFv2 ROUTER OSPFv3 for OSPFv3													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1.(0.0)</td><td>Introduced support for OSPFv3 on the S4810 and Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>7.8.1.0</td><td>Added support for the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Added support for the C-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.													
8.3.19.0	Introduced on the S4820T.													
7.8.1.0	Added support for the C-Series.													
7.4.1.0	Introduced on the E-Series.													
Usage Information	You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique. If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.													
Related Commands	clear ipv6 ospf process – resets an OSPFv3 router process.													

show crypto ipsec policy

Display the configuration of IPsec authentication and encryption policies.

Z9500

Syntax	show crypto ipsec policy [<i>name name</i>]
Parameters	name <i>name</i> (OPTIONAL) Displays configuration details about a specified policy.
Defaults	No default behavior or values.
Command Modes	EXEC EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

Related Commands [show crypto ipsec sa ipv6](#)— displays the IPsec security associations used on OSPFv3 interfaces.

Example

```
Dell#show crypto ipsec policy

Crypto IPSec client security policy data

Policy name : OSPFv3-1-502
Policy refcount : 1
Inbound ESP SPI : 502 (0x1F6)
Outbound ESP SPI : 502 (0x1F6)
Inbound ESP Auth Key : 123456789a123456789b123456789c12
Outbound ESP Auth Key : 123456789a123456789b123456789c12
Inbound ESP Cipher Key :
```

```

123456789a123456789b123456789c123456789d12345678
Outbound ESP Cipher Key :
123456789a123456789b123456789c123456789d12345678
Transform set : esp-3des esp-md5-hmac

Crypto IPsec client security policy data

Policy name : OSPFv3-0-501
Policy refcount : 1
Inbound ESP SPI : 501 (0x1F5)
Outbound ESP SPI : 501 (0x1F5)
Inbound ESP Auth Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97
eb7c0
c30808825fb5
Outbound ESP Auth Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97
eb7c0
c30808825fb5
Inbound ESP Cipher Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8
a
Outbound ESP Cipher Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8
a
Transform set : esp-128-aes esp-sha1-hmac

```

show crypto ipsec policy Command Fields

Field	Description
Policy name	Displays the name of an IPsec policy.
Policy refcount	Number of interfaces on the router that use the policy.
Inbound ESP SPI	The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.
Outbound ESP SPI	
Inbound ESP Auth Key	The ESP authentication key for inbound and outbound links.
Outbound ESP Auth Key	
Inbound ESP Cipher Key	The ESP encryption key for inbound and outbound links.
Outbound ESP Cipher Key	
Transform set	The set of security protocols and algorithms used in the policy.
Inbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound and outbound links.
Outbound AH SPI	
Inbound AH Key	The AH key for inbound and outbound links.
Outbound AH Key	

show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

Z9500

Syntax	<code>show crypto ipsec sa ipv6 [interface <i>interface</i>]</code>											
Parameters	interface <i>interface</i>	(OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where <i>interface</i> is one of the following values: • For a Port Channel interface, enter <code>port-channel <i>number</i></code>. • For a 10-Gigabit Ethernet interface, enter <code>TenGigabitEthernet <i>slot/port</i></code>. • For a 40-Gigabit Ethernet interface, enter <code>fortyGigE <i>slot/port</i></code>. • For a VLAN interface, enter <code>vlan <i>vlan-id</i></code>. The valid VLAN IDs range is from 1 to 4094.										
Defaults	No default behavior or values.											
Command Modes	EXEC EXEC Privilege											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.1.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>8.4.2.0</td><td>Introduced on the E-Series TeraScale.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1.(0.0)	Introduced on the S4810 and Z9000.	8.4.2.0	Introduced on the E-Series TeraScale.	8.3.19.0	Introduced on the S4820T.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
9.1.(0.0)	Introduced on the S4810 and Z9000.											
8.4.2.0	Introduced on the E-Series TeraScale.											
8.3.19.0	Introduced on the S4820T.											
Usage Information	The <code>show crypto ipsec sa ipv6</code> command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.											
Related Commands	show crypto ipsec policy – displays the configuration of IPsec authentication and encryption policies.											

Example

```
Dell#show crypto ipsec policy
Dell#show crypto ipsec sa ipv6

Interface: TenGigabitEthernet 0/0
Link Local address: fe80::201:e8ff:fe40:4d10
IPSecv6 policy name: OSPFv3-1-500

inbound ah sas
spi : 500 (0x1f4)
transform : ah-md5-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE

outbound ah sas
spi : 500 (0x1f4)
transform : ah-md5-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE

inbound esp sas

outbound esp sas

Interface: TenGigabitEthernet 0/1
Link Local address: fe80::201:e8ff:fe40:4d11
IPSecv6 policy name: OSPFv3-1-600

inbound ah sas

outbound ah sas

inbound esp sas
spi : 600 (0x258)
transform : esp-des esp-sha1-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE

outbound esp sas
spi : 600 (0x258)
transform : esp-des esp-sha1-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE
```

show crypto ipsec sa ipv6 Command Fields

Field	Description
Interface	IPv6 interface
Link local address	IPv6 address of interface
IPSecv6 policy name	Name of the IPsec security policy applied to the interface.

inbound/outbound ah	Authentication policy applied to inbound or outbound traffic.
inbound/outbound esp	Encryption policy applied to inbound or outbound traffic.
spi	Security policy index number used to identify the policy.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (only transport mode is supported).
replay detection support	Y: An SA has enabled the replay detection feature. N: The replay detection feature is not enabled.
STATUS	ACTIVE: The authentication or encryption policy is enabled on the interface.

show ipv6 ospf interface

View OSPFv3 interface information.

Z9500

Syntax	<code>show ipv6 ospf [<i>interface</i>]</code>	
Parameters	<i>interface</i>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> and the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> and the slot/port information. - For a Port Channel interface, enter the keywords <code>port-channel</code> and a number. The range is from 1 to 128. - For a Tunnel interface, enter the keywords <code>tunnel</code> and a number. The range is from 1 to 16383. - For a VLAN, enter the keyword <code>vlan</code> and a number from 1 to 4094.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	9.2.(0.0)	Added support for showing BFD status on the S4820T, S4810, and Z9000.
	9.1.(0.0)	Added support for OSPFv3 on the S4810 and Z9000.
	8.3.19.0	Introduced on the S4820T.
	7.8.1.0	Added support for the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	If you enable BFD at the global level, <i>show ipv6 ospf interface</i> shows the BFD provisioning.	
	If you enable BFD at the interface level, <i>show ipv6 ospf interface</i> shows the BFD interval timers.	
Example	<pre> Dell#show ipv6 ospf interface tengigabitethernet 1/0 TenGigabitEthernet 1/0 is up, line protocol is up Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217 Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1 NetworkType BROADCAST, Cost: 1, Passive: No Transmit Delay is 100 sec, State DR, Priority 1 Interface is using OSPF global mode BFD configuration. Designated router on this network is 11.1.1.1 (local) No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5 Dell# </pre>	

show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

Z9500

Syntax	<code>show ipv6 ospf database [database-summary grace-lsa]</code>	
Parameters	database-summary	(OPTIONAL) Enter the keywords <code>database-summary</code> to view a summary of database LSA information.
	grace-lsa	(OPTIONAL): Enter the keywords <code>grace-lsa</code> to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.
Defaults	none	

Command Modes	EXEC EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.1(0.0)</td><td>Added support for OSPFv3 on the S4810 and Z9000.</td></tr> <tr> <td>8.4.2.2</td><td>Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series TeraScale routers.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>7.8.1.0</td><td>Added support for C-Series.</td></tr> </tbody> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	9.1(0.0)	Added support for OSPFv3 on the S4810 and Z9000.	8.4.2.2	Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series TeraScale routers.	8.3.19.0	Introduced on the S4820T.	7.8.1.0	Added support for C-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
9.1(0.0)	Added support for OSPFv3 on the S4810 and Z9000.												
8.4.2.2	Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series TeraScale routers.												
8.3.19.0	Introduced on the S4820T.												
7.8.1.0	Added support for C-Series.												
Usage Information	The <code>show crypto ipsec sa ipv6</code> command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.												
Related Commands	<code>show crypto ipsec policy</code> – displays the configuration of IPsec authentication and encryption policies.												
Example (grace-lsa)	<pre> Dell#show ipv6 ospf database grace-lsa ! Type-11 Grace LSA (Area 0) LS Age : 10 Link State ID : 6.16.192.66 Advertising Router : 100.1.1.1 LS Seq Number : 0x80000001 Checksum : 0x1DF1 Length : 36 Associated Interface : Te 0/3 Restart Interval : 180 Restart Reason : Switch to Redundant Processor </pre>												
Example (database-summary)	<pre> Dell#show ipv6 ospf database database-summary OSPFv3 Router with ID (1.1.1.1) (Process ID 1) Process 1 database summary Type Count/Status Oper Status 1 Admin Status 1 Area Bdr Rtr Status 1 AS Bdr Rtr Status 1 AS Scope LSA Count 0 AS Scope LSA Cksum sum 0 Originate New LSAS 50 </pre>												

```

Rx New LSAS                22
Ext LSA Count               0
Rte Max Eq Cost Paths      10
GR grace-period            180
GR mode                    planned and unplanned

```

```

Area 0 database summary
Type          Count/Status
Brd Rtr Count          1
AS Bdr Rtr Count      1
LSA count             6
Rtr LSA Count         2
Net LSA Count         1
Inter Area Pfx LSA Count 1
Inter Area Rtr LSA Count 0
Group Mem LSA Count    0
Type-7 LSA count      0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count 2

```

```

Area 1 database summary
Type          Count/Status
Brd Rtr Count          1
AS Bdr Rtr Count      1
LSA count             8
Rtr LSA Count         1
Net LSA Count         0
Inter Area Pfx LSA Count 5
Inter Area Rtr LSA Count 0
Group Mem LSA Count    0
Type-7 LSA count      0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count 2

```

```
Dell#show ipv6 ospf neighbor
```

```

Neighbor ID      Pri State          Dead Time Interface ID
Interface
63.114.8.36      1    FULL/DR      00:00:37      4
Te 2/0

```

show ipv6 ospf neighbor

Display the OSPF neighbor information on a per-interface basis.

Z9500

Syntax

```
show ipv6 ospf neighbor [interface]
```

Parameters

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. For the C-Series, Z-Series, and S4810, the range is 1 to 128.

- For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is 1 to 4094.

Defaults none

Command EXEC

Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show ipv6 ospf neighbor te 1/2

Neighbor ID  Pri   State       Dead Time   Interface    ID
Interface
63.114.8.36  1     FULL/DR     00:00:38    4            Te 1/0

Dell#
```

Pay As You Grow

The Pay As You Grow (PAYG) software feature allows you to purchase a Z9500 switch with 36 40G ports (144 10G ports) and upgrade to a larger number of ports as your networking needs grow.

install license

Install the license for Z9500 ports from local flash, a remote server using a file transfer method, or an external flash device.

Z9500

Syntax `install license {flash://filepath | ftp://userid:password@host-ip/filepath | scp://userid:password@hostip/filepath | tftp://host-ip/filepath | usbflash://filepath}`

Parameters

flash://filepath	Enter <code>flash://filepath</code> to install a license from a local flash directory on the switch.
ftp://userid:password@host-ip/filepath	Enter <code>ftp://userid:password@host-ip/filepath</code> to install a license from a remote file server using FTP.
scp://userid:password@hostip/filepath	Enter <code>scp://userid:password@hostip/filepath</code> to install a license from a remote file server using secure copy.
tftp://host-ip/filepath	Enter <code>tftp://host-ip/filepath</code> to install a license from a remote file server using TFTP.
usbflash://filepath	Enter <code>usbflash://filepath</code> to install a license from an external flash device.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.

Usage Information

If your Z9500 switch has a 36 40G-port license, all 40G ports (144 10G ports) on line card 0 are enabled and usable. You can purchase a license to use additional ports:

- 84 40G ports on line cards 0 and 1 (336 10G ports)
- 132 40G ports on line cards 0, 1, and 2 (528 10G ports)

You can upgrade from a 36 40G-port to either an 84 40G-port or 132 40G-port license. You can upgrade from an 84 40G-port to a 132 40G-port license.

In the `install license` command syntax, *host-ip* is either an IPv4 dotted decimal address or an IPv6 [x:x:x:x::x] format address.

An error message is displayed if the license is corrupted or invalid.

Enter `Yes` at the prompt to continue the installation.

You must reload the switch to enable the licensed ports.

Example

```
Dell# install license tftp://10.11.8.12/132.lic
!
3594 bytes successfully copied
Retrieving license ..... (OK)
LICENSE INFORMATION
Vendor           : Dell
Product          : Dell Force10 Z9500
System Service Tag : RthvKsJ
License Service Tag : RTHVKSJ
Feature          : HW-Port-License 132 Ports

Retrieving license data ..... (OK)
Validating license ..... (OK)
Validating Service Tag in license ..... (OK)
```

Note: You must reload the chassis to activate the license.
System will continue to run with current active 84 ports until the next reload !

```
Continue to install license [yes/no]: yes
Installing license ..... (ok)
License installation successful. Restart chassis to activate license
```

```
Dell#Jul 1 11:00:58: %SYSTEM:CP %LICMGR-5-
LICMGR_LIC_INSTALL_SUCCESS: License file install is successful
```

show license

Check the status of a Z9500 license and display the number of usable ports or verify a license stored on a remote server before you install it.

Z9500

Syntax	<code>show license [flash://filepath ftp://userid:password@host-ip/filepath scp://userid:password@hostip/filepath tftp://host-ip/filepath usbflash://filepath]</code>					
Parameters	flash://filepath	Enter <code>flash://filepath</code> to display a license stored in a local flash directory on the switch.				
	ftp://userid:password@host-ip/filepath	Enter <code>ftp://userid:password@host-ip/filepath</code> to display a license stored on a remote file server using FTP.				
	scp://userid:password@hostip/filepath	Enter <code>scp://userid:password@hostip/filepath</code> to display a license stored on a remote file server using secure copy.				
	tftp://host-ip/filepath	Enter <code>tftp://host-ip/filepath</code> to display a license stored on a remote file server using TFTP.				
	usbflash://filepath	Enter <code>usbflash://filepath</code> to display a license stored on an external flash device.				
Defaults	None					
Command Modes	EXEC Privilege					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.
Version	Description					
9.5(0.1)	Introduced on the Z9500.					
Usage Information	In the <code>show license</code> command syntax, <i>host-ip</i> is either an IPv4 dotted decimal address or an IPv6 [x:x:x:x::x] format address. The following examples show sample output.					
Example	If no license is installed, information about the factory-installed 36 40G-port or 132 40G-port configuration is displayed. <pre>Dell# show license LICENSE INFORMATION</pre>					

```
Vendor           : Dell
Product          : Dell Force10 Z950
System Service Tag: RthvKsJ
License Service Tag:
Current State    : HW-Port-License 36 Ports (Fo 0/0-Fo 0/140)
Next Boot        : HW-Port-License 36 Ports (Fo 0/0-Fo 0/140)
```

If an 84 40G-port license is installed, the following information is displayed.

```
Dell# show license
LICENSE INFORMATION
Vendor           : Dell
Product          : Dell Force10 Z9500
System Service Tag: RthvKsJ
License Service Tag: RTHVKSJ
Current State    : HW-Port-License 84 Ports (Fo 0/0-Fo 1/188)
Next Boot        : HW-Port-License 84 Ports (Fo 0/0-Fo 1/188)
```

To verify the license stored on a remote server using TFTP:

```
Dell# show license tftp://10.11.8.12/132.lic
!
3594 bytes successfully copied
LICENSE INFORMATION
Vendor           : Dell
Product          : Dell Force10 Z9500
System Service Tag: RTHVKSJ
License Service Tag: RTHVKSJ
License Type     : HW-Port-License 132 Ports (Fo 0/0-Fo
2/188)
Status           : Valid license file
```

PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast sparse-mode (PIM-SM) commands in this section are supported in the Dell Networking operating system.

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

clear ip pim rp-mapping

The bootstrap router (BSR) feature uses this command to remove all or particular rendezvous point (RP) advertisement.

Z9500

Syntax	<code>clear ip pim rp-mapping <i>rp-address</i></code>	
Parameters	<i>rp-address</i>	(OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

clear ip pim tib

Clear PIM tree information from the PIM database.

Z9500

Syntax	<code>clear ip pim tib [group]</code>	
Parameters	group	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information	If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The local VLT node sends a request to the peer VLT node to download multicast routes learned by the peer. Both local and synced routes are removed from the local VLT node multicast route table. The peer VLT node clears synced routes from the node. If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.
--------------------------	---

debug ip pim

View IP PIM debugging messages.

Z9500

Syntax	<code>debug ip pim [bsr events group packet [in out] register state timer [assert hello joinprune register]]</code>
---------------	---

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all` to disable all debugging command.

Parameters

bsr	(OPTIONAL) Enter the keyword <code>bsr</code> to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
packet [in out]	(OPTIONAL) Enter the keyword <code>packet</code> to view PIM packets. Enter one of the optional parameters: • <code>in</code>: to view incoming packets • <code>out</code>: to view outgoing packets
register	(OPTIONAL) Enter the keyword <code>register</code> to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword <code>state</code> to view PIM state changes.
timer [assert hello joinprune register]	(OPTIONAL) Enter the keyword <code>timer</code> to view PIM timers. Enter one of the optional parameters: • <code>assert</code>: to view the assertion timer • <code>hello</code>: to view the PIM neighbor keepalive timer • <code>joinprune</code>: to view the expiry timer (join/prune timer) • <code>register</code>: to view the register suppression timer

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

ip pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Z9500

Syntax	<pre>ip pim bsr-border</pre> To return to the default value, use the <code>no ip pim bsr-border</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information	This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time-out. To clean the candidate RP advertisements, use the <code>clear ip pim rp-mapping</code> command.
--------------------------	---

ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

Z9500

Syntax	<pre>ip pim bsr-candidate interface [hash-mask-length] [priority]</pre> To return to the default value, use the <code>no ip pim bsr-candidate</code> command.
---------------	--

Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 1-Gigabit Ethernet interface, enter the keyword <code>Gigabit</code> then the slot/port information. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>hash-mask-length</i>	(OPTIONAL) Enter the hash mask length. The range is from zero (0) to 32. The default is 30 .
	<i>priority</i>	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is zero (0) .

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.1.1.0	Added support for the VLAN interface.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

Z9500

Syntax	<code>ip pim dr-priority <i>priority-value</i></code> To remove the DR priority value assigned, use the <code>no ip pim dr-priority</code> command.																	
Parameters	<i>priority-value</i>	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.																
Defaults	1																	
Command Modes	INTERFACE																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series on port-channels and the S-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the C-Series on port-channels and the S-Series.
Version	Description																	
9.5(0.1)	Introduced on the Z9500.																	
9.0.2.0	Introduced on the S6000.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
8.1.1.0	Introduced on the E-Series ExaScale.																	
7.8.1.0	Introduced on the C-Series on port-channels and the S-Series.																	
Usage Information	The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.																	

ip pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

Z9500

Syntax	<code>ip pim join-filter <i>ext-access-list</i> {in out}</code>
---------------	---

To remove the access list, use the `no ip pim join-filter ext-access-list {in | out}` command.

Parameters

<code>ext-access-list</code>	Enter the name of an extended access list.
<code>in</code>	Enter this keyword to apply the access list to inbound traffic.
<code>out</code>	Enter this keyword to apply the access list to outbound traffic.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.
7.7.1.0	Introduced on the E-Series.

Example

```
Dell(conf)# ip access-list extended iptv-channels
Dell(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
Dell(config-ext-nacl)# permit ip any 232.1.1.0/24
Dell(config-ext-nacl)# permit ip 100.1.1.0/16 any
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels in
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels out
```

Related Commands

[ip access-list extended](#) — configure an access list based on IP addresses or protocols.

ip pim ingress-interface-map

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

Z9500

Syntax	<code>ip pim ingress-interface-map <i>std-access-list</i></code>	
Parameters	<i>std-access-list</i>	Enter the name of a standard access list.
Defaults	none	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced

Example	<pre>Dell(conf)# ip access-list standard map1 Dell(config-std-nacl)# permit 224.0.0.1/24 Dell(config-std-nacl)#exit Dell(conf)#int tengig 1/1 Dell(config-if-te-1/1)# ip pim ingress-interface-map map1</pre>
---------	---

ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

Z9500

Syntax	<code>ip pim neighbor-filter {<i>access-list</i>}</code> To remove the restriction, use the <code>no ip pim neighbor-filter {<i>access-list</i>}</code> command.	
Parameters	<i>access-list</i>	Enter the name of a standard access list. Maximum 16 characters.
Defaults	none	

Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the C-Series and S-Series.	7.6.1.0	Introduced on the E-Series.
Version	Description																		
9.5(0.1)	Introduced on the Z9500.																		
9.0.2.0	Introduced on the S6000.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.8.1.0	Introduced on the C-Series and S-Series.																		
7.6.1.0	Introduced on the E-Series.																		
Usage Information	Do not enter this command before creating the access-list.																		

ip pim query-interval

Change the frequency of PIM Router-Query messages.

Z9500

Syntax	<pre>ip pim query-interval seconds</pre> To return to the default value, use the <code>no ip pim query-interval seconds</code> command.	
Parameters	seconds	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is 30 seconds .
Defaults	30 seconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.

ip pim register-filter

To prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group, use this feature.

Z9500

Syntax `ip pim register-filter access-list`
To return to the default, use the `no ip pim register-filter access-list` command.

Parameters

<i>access-list</i>	Enter the name of an extended access list. Maximum 16 characters.
---------------------------	---

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced

Usage Information	The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.
--------------------------	--

ip pim rp-address

Configure a static PIM rendezvous point (RP) address for a group or access-list.

Z9500

Syntax	<code>ip pim rp-address address {group-address group-address mask} override</code> To remove an RP address, use the <code>no ip pim rp-address address {group-address group-address mask} override</code> command.
---------------	---

Parameters	address	Enter the RP address in dotted decimal format (A.B.C.D).
	group-address group-address mask	Enter the keywords <code>group-address</code> then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
	override	Enter the keyword <code>override</code> to override the BSR updates with static RP. The override takes effect immediately during enable/disable.
	 NOTE: This option is applicable to multicast group range.	

Defaults	Not configured.																		
Command Modes	CONFIGURATION																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the S-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																		
9.5(0.1)	Introduced on the Z9500.																		
9.0.2.0	Introduced on the S6000.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.1.1.0	Introduced on the E-Series ExaScale.																		
7.8.1.0	Introduced on the S-Series.																		
6.1.1.1	Introduced on the E-Series.																		

Usage Information	First-hop routers use this address by to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned using BSR take priority over static RP addresses. Without the <code>override</code> option, RPs advertised by the BSR updates take precedence over the statically configured RPs.
--------------------------	--

ip pim rp-candidate

To send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR, configure a PIM router.

Z9500

Syntax	<code>ip pim rp-candidate {<i>interface</i> [<i>priority</i>]}</code> To return to the default value, use the <code>no ip pim rp-candidate {<i>interface</i> [<i>priority</i>]}</code> command.
---------------	--

Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 1-Gigabit Ethernet interface, enter the keyword <code>Gigabit</code> then the slot/port information. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>priority</i>	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is 192 .

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

Z9500

Syntax	<code>ip pim sparse-mode</code> To disable PIM sparse mode and IGMP, use the <code>no ip pim sparse-mode</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.

Usage Information The interface must be enabled (the `no shutdown` command) and not have the `switchport` command configured. Multicast must also be enabled globally (using

the `ip multicast-lag-hashing` command). PIM is supported on the port-channel interface.

ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources, or for a specific set of (S,G) pairs an access list defines.

Z9500

Syntax `ip pim sparse-mode sg-expiry-timer seconds [access-list name]`
To disable configured timers and return to default mode, use the `no ip pim sparse-mode sg-expiry-timer` command.

Parameters

seconds	Enter the number of seconds the S, G entries are retained. The range is from 211 to 86400.
access-list name	(OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries.

Defaults Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.
7.7.1.1	Introduced

Usage Information This command configures an expiration timer for all S,G entries, unless they are assigned to an Extended ACL.

ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

Z9500

Syntax	<code>ip pim spt-threshold value infinity</code>	
	To return to the default value, use the <code>no ip pim spt-threshold</code> command.	
Parameters	value	(OPTIONAL) Enter the traffic value in kilobits per second. The default is 10 packets per second . A value of zero (0) causes a switchover on the first packet.
	infinity	(OPTIONAL) Enter the keyword <code>infinity</code> to never switch to the source-tree.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.12.0	Introduced on the S4810.
	8.1.1.0	Introduced on the E-Series ExaScale.
Usage Information	This command is applicable to last hop routers on the shared tree towards the rendezvous point (RP).	

no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

Z9500

Syntax	<code>no ip pim snooping dr-flood</code>	
	To re-enable the flooding of multicast packets to the PIM designated router, use the <code>ip pim snooping dr-flood</code> command.	
Defaults	Enabled.	

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced on the E-Series ExaScale.

Usage Information

By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable `designated-router flooding`.

When designated-router flooding is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router.

If the PIM DR flood is not disabled (default setting):

- Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.
- Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.

show ip pim bsr-router

View information on the Bootstrap router.

Z9500

Syntax

```
show ip pim bsr-router
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask
length: 30
```

show ip pim interface

View information on the interfaces with IP PIM enabled.

Z9500

Syntax show ip pim interface

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

The following describes the `show ip pim interface` command shown in the following example.

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with <code>ip pim query-interval</code> command).
DR Prio	Displays the Designated Router priority value configured on the interface (use the <code>ip pim dr-priority</code> command).
DR	Displays the IP address of the Designated Router for that interface.

Example

```
Dell#show ip pim interface
Address      Interface  Ver/  Nbr   Query  DR    DR
              Mode Count Intvl Prio
172.21.200.254 Te 0/9    v2/S  0     30 1   172.21.200.254
172.60.1.2    Te 0/11   v2/S  0     30 1   172.60.1.2
192.3.1.1     Te 0/16   v2/S  1     30 1   192.3.1.1
192.4.1.1     Te 1/5    v2/S  0     30 1   192.4.1.1
172.21.110.1  Te 1/6    v2/S  0     30 1   172.21.110.1
172.21.203.1  Te 1/7    v2/S  0     30 1   172.21.203.1
```

show ip pim neighbor

View PIM neighbors.

Z9500

Syntax

```
show ip pim neighbor
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

The following describes the `show ip pim neighbor` command shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number. v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. 1 = default Designated Router priority (use the <code>ip pim dr-priority</code> command) - DR = Designated Router - S = Sparse mode

Example

```
Dell#show ip pim neighbor
Neighbor  Interface  Uptime/Expires    Ver  DR
Address                                     Prio/Mode
127.87.3.4 Te 1/16    09:44:58/00:01:24  v2   1 / S
Dell#
```

show ip pim rp

View all multicast groups-to-RP mappings.

Z9500

Syntax	show ip pim rp [mapping group-address]	
Parameters	mapping	(OPTIONAL) Enter the keyword <code>mapping</code> to display the multicast groups-to-RP mapping and information on how RP is learnt.
	group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example	Dell#show ip pim rp
	Group RP
	224.2.197.115 165.87.20.4
	224.2.217.146 165.87.20.4
	224.3.3.3 165.87.20.4
	225.1.2.1 165.87.20.4
	225.1.2.2 165.87.20.4
	229.1.2.1 165.87.20.4
	229.1.2.2 165.87.20.4
	Dell#

Example (Mapping)	Dell#show ip pim rp mapping
	Group(s): 224.0.0.0/4
	RP: 165.87.20.4, v2
	Info source: 165.87.20.5, via bootstrap, priority 0
	Uptime: 00:03:11, expires: 00:02:46
	RP: 165.87.20.3, v2

```
Info source: 165.87.20.5, via bootstrap, priority 0
Uptime: 00:03:11, expires: 00:03:03
```

Example
(Address)

```
Dell#show ip pim rp 229.1.2.1
Group      RP
229.1.2.1  165.87.20.4
```

show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

Z9500

Syntax `show ip pim snooping interface [vlan vlan-id]`

Parameters

vlan *vlan-id* (OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN IDs range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.1	Introduced on the E-Series ExaScale.

Usage Information

The following describes the `show ip pim snooping interface` commands shown in the following example.

Field	Description
Interface	Displays the VLAN interfaces with PIM-SM snooping enabled.
Ver/Mode	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: • v2 = PIM version 2 • S = PIM Sparse mode

Field	Description
Nbr Count	Displays the number of neighbors learned through PIM-SM snooping on the interface.
DR Prio	Displays the Designated Router priority value configured on the interface (<code>ip pim dr-priority</code> command).
DR	Displays the IP address of the Designated Router for that interface.

Example (#2)

```
Dell#show ip pim snooping interface
Interface Ver Nbr    DR    DR
          Count Prio
Vlan 2    v2  3     1    165.87.32.2
```

show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

Z9500

Syntax	<code>show ip pim snooping neighbor [vlan <i>vlan-id</i>]</code>
Parameters	vlan <i>vlan-id</i> (OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.
Command Modes	- EXEC - EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.1	Introduced on the E-Series ExaScale.

Usage Information	The following describes the <code>show ip pim snooping neighbor</code> commands shown in the following example.
-------------------	---

Field	Description
Neighbor address	Displays the IP address of the neighbor learned through PIM-SM snooping.

Field	Description
Interface	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number: v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode: 1 = default Designated Router priority (use the <code>ip pim dr-priority</code> command) - DR = Designated Router - S = Sparse mode

Example

```
Dell#show ip pim snooping neighbor
```

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Prio
165.87.32.2	Vl 2 [Te 1/13]	00:04:03/00:01:42	v2	1	
165.87.32.10	Vl 2 [Te 1/11]	00:00:46/00:01:29	v2	0	
165.87.32.12	Vl 2 [Te 41/20]	00:00:51/00:01:24	v2	0	

show ip pim snooping tib

Display information from the tree information base (TIB) PIM-SM snooping discovered about multicast group members and states.

Z9500

Syntax `show ip pim snooping tib [vlan vlan-id] [group-address [source-address]]`

Parameters

<i>vlan <i>vlan-id</i></i>	(OPTIONAL) Enter a VLAN ID to display TIB information PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.
<i>group-address</i>	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast group.
<i>source-address</i>	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast source.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.1	Introduced on the E-Series ExaScale.

Usage Information

The following describes the `show ip pim snooping tib` commands shown in the following example.

Field	Description
(S, G)	Displays the entry in the PIM multicast snooping database.
uptime	Displays the amount of time the entry has been in the PIM multicast route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K=acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/ source.

Field	Description
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
Dell#show ip pim snooping tib

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
      SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(*, 225.1.2.1), uptime 00:00:01, expires 00:02:59, RP
165.87.70.1, flags: J
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet 2/11 RPF 165.87.32.2 00:00:01/00:02:59
    TenGigabitEthernet 2/13 Upstream Port -/-

Dell#show ip pim snooping tib vlan 2 225.1.2.1 165.87.1.7

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
      SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(165.87.1.7, 225.1.2.1), uptime 00:00:08, expires 00:02:52,
flags: j
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet 2/11 Upstream Port -/-
    TenGigabitEthernet 2/13 DR Port -/-
    TenGigabitEthernet 2/20 RPF 165.87.32.10 00:00:08/00:02:52
```

show ip pim summary

View information about PIM-SM operation.

Z9500

Syntax `show ip pim summary`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.1	Support for the display of PIM-SM snooping status was added on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example

```

Dell# show ip pim summary

PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2

Active Modes :
    PIM-SNOOPING

Interface summary:
    1 active PIM interface
    0 passive PIM interfaces
    3 active PIM neighbors

TIB summary:
    1/1 (*,G) entries in PIM-TIB/MFC
    1/1 (S,G) entries in PIM-TIB/MFC
    0/0 (S,G,Rpt) entries in PIM-TIB/MFC

    0 PIM nexthops
    0 RPs
    0 sources
    0 Register states

Message summary:
    2582/2583 Joins sent/received
    5/0 Prunes sent/received
    0/0 Candidate-RP advertisements sent/received
    0/0 BSR messages sent/received
    0/0 State-Refresh messages sent/received
    0/0 MSDP updates sent/received
    0/0 Null Register messages sent/received
    0/0 Register-stop messages sent/received

Data path event summary:
    0 no-cache messages received
    0 last-hop switchover messages received
    0/0 pim-assert messages sent/received
    0/0 register messages sent/received

Memory usage:
    TIB : 3768 bytes
    Nexthop cache : 0 bytes
    Interface table : 992 bytes

```

Neighbor table : 528 bytes
RP Mapping : 0 bytes

show ip pim tib

View the PIM tree information base (TIB).

Z9500

Syntax	show ip pim tib [<i>group-address</i> [<i>source-address</i>]]																	
Parameters	<i>group-address</i>	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).																
	<i>source-address</i>	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).																
Command Modes	- EXEC - EXEC Privilege																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the S-Series.
Version	Description																	
9.5(0.1)	Introduced on the Z9500.																	
9.0.2.0	Introduced on the S6000.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.12.0	Introduced on the S4810.																	
8.3.11.1	Introduced on the Z9000.																	
8.1.1.0	Introduced on the E-Series ExaScale.																	
7.8.1.0	Introduced on the S-Series.																	
Usage Information	The following describes the show ip pim tib command shown in the following example. <table><tr><th>Field</th><th>Description</th></tr><tr><td>(S, G)</td><td>Displays the entry in the multicast PIM database.</td></tr><tr><td>uptime</td><td>Displays the amount of time the entry has been in the PIM route table.</td></tr><tr><td>expires</td><td>Displays the amount of time until the entry expires and is removed from the database.</td></tr><tr><td>RP</td><td>Displays the IP address of the RP/source for this entry.</td></tr></table>		Field	Description	(S, G)	Displays the entry in the multicast PIM database.	uptime	Displays the amount of time the entry has been in the PIM route table.	expires	Displays the amount of time until the entry expires and is removed from the database.	RP	Displays the IP address of the RP/source for this entry.						
Field	Description																	
(S, G)	Displays the entry in the multicast PIM database.																	
uptime	Displays the amount of time the entry has been in the PIM route table.																	
expires	Displays the amount of time until the entry expires and is removed from the database.																	
RP	Displays the IP address of the RP/source for this entry.																	

Field	Description
flags	List the flags to define the entries: • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/ source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
Dell#show ip pim tib

PIM Multicast Routing Table
Flags:D- Dense, S- Sparse, C- Connected, L- Local, P- Pruned,
      R- RP-bit set, F- Register flag, T- SPT-bit set, J- Join
SPT,
      M- MSDP created entry, A- Candidate for MSDP
Advertisement,
      K- Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 0/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 1/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
  Incoming interface: TenGigabitEthernet 0/23, RPF neighbor
10.211.1.2
  Outgoing interface list:
    GigabitEthernet 1/0
```

```

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
    Incoming interface: TenGigabitEthernet 0/23, RPF neighbor
10.211.1.2
    Outgoing interface list:
        TenGigabitEthernet 1/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP
10.211.2.1, flags: SCJ
    Incoming interface: TenGigabitEthernet 0/23, RPF neighbor
10.211.1.2
    Outgoing interface list:
        TenGigabitEthernet 1/0

```

show running-config pim

Display the current configuration of PIM-SM snooping.

Z9500

Syntax	show running-config pim
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the E-Series ExaScale.

Example	Dell#show running-config pim ! ip pim snooping enable
---------	---

IPv6 PIM-Sparse Mode Commands

The following describes the IPv6 PIM-sparse mode (PIM-SM) commands.

clear ipv6 pim tib

Clear the IPv6 PIM multicast-routing database (tree information base-TIB).

Z9500

Syntax	<code>clear ipv6 pim tib [group-address]</code>	
Parameters	group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x:x format.
		NOTE: The :: notation specifies successive hexadecimal fields of zero.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.0.2.0	Introduced on the S6000.
	9.0(1.3)	Introduced on the S5000.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
Related Commands	show ipv6 pim tib – displays the IPv6 PIM tree information base (TIB)	

ipv6 pim bsr-border

Invoke IPv6 PIM debugging.

Z9500

Syntax	<code>debug ipv6 pim [bsr events group group packet register [group] state timer [assert hello joinprune register]]</code> To disable IPv6 PIM debugging, use the <code>no debug ipv6 pim</code> command.	
Parameters	bsr	(OPTIONAL) Enter the keyword <code>bsr</code> to invoke debugging of IPv6 PIM Candidate RP/BSR activities.
	events	(OPTIONAL) Enter the keyword <code>events</code> to invoke debugging of IPv6 PIM events.

group <i>group</i>	(OPTIONAL) Enter the keyword <code>group</code> then the group address to invoke debugging on that specific group.										
packet	(OPTIONAL) Enter the keyword <code>packet</code> to invoke debugging of IPv6 PIM packets.										
register [<i>group</i>]	(OPTIONAL) Enter the keyword <code>register</code> and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.										
state	(OPTIONAL) Enter the keyword <code>state</code> to view IPv6 PIM state changes.										
timer [<i>assert</i> <i>hello</i> <i>joinprune</i> <i>register</i>]	(OPTIONAL) Enter the keyword <code>timer</code> to view IPv6 PIM timers. Enter one of the optional parameters: • <code>assert</code>: to view the assertion timer • <code>hello</code>: to view the IPv6 PIM neighbor keepalive timer • <code>joinprune</code>: to view the expiry timer (join/prune timer) • <code>register</code>: to view the register suppression timer										
Defaults	Disabled.										
Command Modes	EXEC Privilege										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	7.4.1.0	Introduced
Version	Description										
9.5(0.1)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.12.0	Introduced on the S4810.										
7.4.1.0	Introduced										

ipv6 pim bsr-candidate

Configure the router as a bootstrap (BSR) candidate.

Z9500

Syntax	<pre>ipv6 pim bsr-candidate <i>interface</i> [<i>hash-mask-length</i>] [<i>priority</i>]</pre> To disable the bootstrap candidate, use the <code>no ipv6 pim bsr-candidate</code> command.
Parameters	<i>interface</i> Enter the following keywords and slot/port or number information:

	- For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
	<i>hash-mask-length</i> (OPTIONAL) Enter the hash mask length for RP selection. The range is from 0 to 128. The default is 126. <i>priority</i> (OPTIONAL) Enter the priority value for Bootstrap election process. The range is from 0 to 255. The default is 0.
Defaults	Refer to Parameters.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

Z9500

Syntax	<pre>ipv6 pim dr-priority <i>priority-value</i></pre> To remove the DR priority value assigned, use the <code>no ipv6 pim dr-priority</code> command.	
Parameters	<i>priority-value</i>	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1 .
Defaults	1	

Command Modes	INTERFACE										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	7.4.1.0	Introduced
Version	Description										
9.5(0.1)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.12.0	Introduced on the S4810.										
7.4.1.0	Introduced										
Usage Information	The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.										

ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

Z9500

Syntax	ipv6 pim join-filter <i>access-list</i>							
Parameters	<i>access-list</i>	Enter the name of an extended access list.						
	in	Enter the keyword <code>in</code> to apply the access list to inbound traffic.						
	out	Enter the keyword <code>out</code> to apply the access list to outbound traffic.						
Defaults	none							
Command Modes	INTERFACE							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

Version	Description
8.3.12.0	Introduced on the S4810.
7.3.1.0	Introduced

Example

```
Dell(config)#ipv6 access-list JOIN-FIL_ACL
Dell(config-ipv6-acl)#permit ipv6 165:87:34::0/112 ff0e::
225:1:2:0/112
Dell(config-ipv6-acl)#permit ipv6 any ff0e::230:1:2:0/112
Dell(config-ipv6-acl)#permit ipv6 165:87:32::0/112 any
Dell(config-ipv6-acl)#exit
Dell(config)#interface tengigabitethernet 0/84
Dell(config-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL in
Dell(config-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL out
```

ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

Z9500

Syntax	ipv6 pim neighbor-filter { <i>access-list</i> }
Parameters	<i>access-list</i> Enter the name of a standard access list. Maximum 16 characters.
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.1.0	Introduced

Usage Information	Do not enter this command before creating the access-list.
-------------------	--

ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

Z9500

Syntax `ipv6 pim query-interval seconds`
To return to the default value, use the `no ipv6 pim query-interval seconds` command.

Parameters **seconds** Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

Z9500

Syntax `ipv6 pim register-filter access-list`

Parameters **access-list** Enter the name of the extended ACL that contains the sources and groups to filter.

Defaults none

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.1.0	Introduced

Example

```
Dell(conf)#ipv6 pim register-filter REG-FIL_ACL
Dell(conf)#ipv6 access-list REG-FIL_ACL
Dell(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::
225:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 any any
Dell(conf-ipv6-acl)#exit
```

ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. First-hop routers use this address to send register packets on behalf of the source multicast host.

Z9500

Syntax

```
ipv6 pim rp-address address group-address group-address mask
override
```

To remove an RP address, use the `no ipv6 pim re-address address group-address mask override` command.

Parameters

address

Enter the IPv6 RP address in the x:x:x:x:x format.



NOTE: The :: notation specifies successive hexadecimal fields of zero.

group-address group-address mask

Enter the keywords `group-address` then the group address in the x:x:x:x:x format and then the mask in /nn format to assign that group address to the RP.



NOTE: The :: notation specifies successive hexadecimal fields of zero.

override

Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable.



NOTE: This option is applicable to multicast group range.

Defaults	none										
Command Modes	CONFIGURATION										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	7.4.1.0	Introduced
Version	Description										
9.5(0.1)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.12.0	Introduced on the S4810.										
7.4.1.0	Introduced										
Usage Information	The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses. Without the override option, the BSR-advertised RPs updates take precedence over the statically configured RPs.										

ipv6 pim rp-candidate

Specify an interface as an RP candidate.

Z9500

Syntax	<code>ipv6 pim rp-candidate interface [priority-value]</code>	
Parameters	interface Enter the following keywords and slot/port or number information: - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.	
	priority-value (OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements. The range is 0 (highest) to 255 (lowest).	

Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode on the interface.

Z9500

Syntax	<code>ipv6 pim sparse-mode</code> To disable IPv6 PIM sparse mode, use the <code>no ipv6 pim sparse-mode</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Usage Information	Enable the interface (use the <code>no shutdown</code> command) and not have the <code>switchport</code> command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.
--------------------------	--

ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

Z9500

Syntax `ipv6 pim spt-threshold {kbps | infinity}`
To return to the default value, use the `no ipv6 pim spt-threshold` command.

Parameters

kbps	Enter a traffic rate in kilobytes per second. The range is from 0 to 4294967 kbps. The default is 10 kbps .
infinity	Enter the keyword <code>infinity</code> to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

Defaults **10 kbps**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Usage Information PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

show ipv6 pim bsr-router

View information on the bootstrap router (v2).

Z9500

Syntax `show ipv6 pim bsr-router`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Example

```
Dell#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 14::2
  Uptime: 00:02:54, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:06

This system is a candidate BSR
  Candidate BSR address: 14::2, priority: 0, hash mask length:
126
Dell#
```

show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

Z9500

Syntax

```
show ipv6 pim interface
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Example

```
Dell#show ipv6 pim interface
Interface Ver/ Nbr  Query DR
          Mode Count Intvl Prio
```

```

Te 1/3   v2/S 1       30    1
  Address : fe80::201:e8ff:fe02:140f
  DR : this router

Te 1/11  v2/S 0       30    1
  Address : fe80::201:e8ff:fe02:1417
  DR : this router
Dell#

```

show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

Z9500

Syntax	show ipv6 pim neighbor [detail]		
Parameters	detail	(OPTIONAL) Enter the keyword <code>detail</code> to displayed PIM neighbor detailed information.	
Command Modes	- EXEC - EXEC Privilege		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.		

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Example	<pre> Dell#show ipv6 pim neighbor detail Neighbor Interface Uptime/Expires Ver DR Address Prio/Mode fe80::201:e8ff:fe00:6265 Gi 10/3 00:07:39/00:01:42 v2 1 / S 165:87:50::6 Dell# </pre>
----------------	---

show ipv6 pim rp

View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

Z9500

Syntax	show ipv6 pim rp [mapping <i>group-address</i>]
---------------	--

Parameters

- mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learned.
- group-address** (OPTIONAL) Enter the multicast group address in the `x::x::x::x` format to view RP mappings for a specific group.
-  **NOTE:** The `::` notation specifies successive hexadecimal fields of zero.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Example

```
Dell#show ipv6 pim rp
Group RP
ff0e::225:1:2:1 14::1
ff0e::225:1:2:2 14::1
ff0e::226:1:2:1 14::1
ff0e::226:1:2:2 14::1
Dell#
```

Example (Mapping)

```
Dell#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 14::1, v2
    Info source: 14::1, via bootstrap, priority 192
    Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
Dell#
```

show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base — tib).

Z9500

Syntax

```
show ipv6 pim tib [group-address [source-address]]
```

Parameters

- group-address*** (OPTIONAL) Enter the multicast group address in the x:x:x:x:x format to view RP mappings for a specific group.
-  **NOTE:** The :: notation specifies successive hexadecimal fields of zero.
- source-address*** (OPTIONAL) Enter the source address in the x:x:x:x:x format.
-  **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0(1.3)	Introduced on the S5000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.4.1.0	Introduced

Example

```
Dell#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P -
Pruned,
      R - RP-bit set, F - Register flag, T - SPT-bit set, J -
Join SPT,
      M - MSDP created entry, A - Candidate for MSDP
Advertisement
      K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires
```

```

00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires
00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires
00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3,
fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11
Dell#

```

Related Commands

[clear ipv6 pim tib](#) – clears the IPv6 PIM tree information base (TIB)

PIM-Source Specific Mode (PIM-SSM)

The protocol-independent multicast source-specific mode (PIM-SSM) commands in this section are supported in the Dell Networking operating system.

IPv4 PIM Commands

The following commands apply to IPv4 PIM-SM, IPv4 PIM-SSM, and PIM-DM.

- [clear ip pim tib](#)
- [debug ip pim](#)
- [ip pim dr-priority](#)
- [ip pim neighbor-filter](#)
- [ip pim query-interval](#)
- [show ip pim interface](#)
- [show ip pim neighbor](#)
- [show ip pim tib](#)

IPv4 PIM-Source Specific Mode Commands

The following IPv4 PIM-source specific mode (PIM-SSM) commands are supported:

- [ip pim ssm-range](#)
- [show ip pim ssm-range](#)

ip pim ssm-range

Specify the SSM group range using an access list.

Z9500

Syntax	<code>ip pim ssm-range {access_list_name}</code>	
Parameters	<i>access_list_name</i>	Enter the name of the access list.

Defaults	Default SSM range is 232/8 and ff3x/32																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.1</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.1	Introduced on the S4810.	8.1.1.0	Introduced on the E-Series ExaScale.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.	7.5.1.0	Introduced on the E-Series.
Version	Description																				
9.5(0.1)	Introduced on the Z9500.																				
9.0.2.0	Introduced on the S6000.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.1	Introduced on the S4810.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.8.1.0	Introduced on the S-Series.																				
7.7.1.0	Introduced on the C-Series.																				
7.5.1.0	Introduced on the E-Series.																				
Usage Information	Dell Networking OS supports standard access lists for the SSM range. You cannot use extended ACLs for configuring the SSM range. If you configure an extended ACL and then used in the <code>ip pim ssm-range {access list name}</code> configuration, an error is reported. However, if you configure <code>ip pim ssm-range {access list name}</code> first and then you configure the ACL as an Extended ACL, an error is not reported and the ACL is not applied to the SSM range. Dell Networking OS-recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. After the SSM range is applied, the changes are applied internally without requiring clearing of the tree information base (TIB). When the ACL rules change, the ACL and protocol-independent multicast (PIM) modules apply the new rules automatically. When you configure the SSM range, Dell Networking OS supports SSM for configured group range as well as the default SSM range. When you remove the SSM ACL, PIM SSM is supported for the default SSM range only.																				

show ip pim ssm-range

Display the non-default groups added using the SSM range feature.

Z9500

Syntax	show ip pim ssm-range	
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	Version 9.5(0.0)	Introduced on the Z9500.
	Version 9.0.2.0	Introduced on the S6000.
	Version 8.3.19.0	Introduced on the S4820T.
	Version 8.3.11.1	Introduced on the Z9000.
	Version 8.3.7.1	Introduced on the S4810.
	Version 8.1.1.0	Introduced on the E-Series ExaScale.
	Version 7.8.1.0	Introduced on the S-Series.
	Version 7.7.1.0	Introduced on the C-Series.
	Version 7.5.1.0	Introduced on the E-Series.

IPv6 PIM Commands

The following commands apply to IPv6 PIM-SM and IPv6 PIM-SSM.

- [clear ipv6 pim tib](#)
- [debug ip pim](#)
- [ipv6 pim dr-priority](#)
- [ipv6 pim join-filter](#)
- [ipv6 pim query-interval](#)
- [ipv6 pim neighbor-filter](#)
- [show ipv6 pim interface](#)
- [show ipv6 pim neighbor](#)
- [show ipv6 pim tib](#)

IPv6 PIM-Source Specific Mode Commands

The following IPv6 PIM-SSM commands are supported:

- [ip pim ssm-range](#)
- [show ipv6 pim ssm-range](#)

ipv6 pim ssm-range

Specify the SSM group range using an access list.

Z9500

Syntax	ipv6 pim ssm-range { <i>access_list_name</i> }							
Parameters	<i>access_list_name</i>	Enter the name of the access list. Maximum 16 characters.						
Defaults	Default SSM range is 232/8 and ff3x/32							
Command Modes	CONFIGURATION							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	7.5.1.0	Introduced on the E-Series.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
7.5.1.0	Introduced on the E-Series.							
Usage Information	After the SSM range is applied, the changes are applied internally without requiring clearing of the TIB. The SSM ACL overrides the default range. To use the default range while the SSM range is active, add the default range to the SSM ACL. When the ACL rules change, the ACL manager and PIM modules apply the new rules automatically. When you remove the SSM ACL, the default range is restored. When you configure the SSM range, the system supports SSM for the configured group range as well as the default SSM range.							

show ipv6 pim ssm-range

Display the non-default groups added using the SSM range feature.

Z9500

Syntax `show ipv6 pim ssm-range`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell(conf)#ipv6 pim ssm-range SSM_ACL
Dell(conf)#ipv6 access-list SSM_ACL
Dell(conf-ipv6-acl)#permit ipv6 any ff0e::225:1:2:0/112
Dell(conf-ipv6-acl)#
Dell(conf-ipv6-acl)#do show ipv6 pim ssm-range
Group Address / MaskLen
ff0e::225:1:2:0 / 112
Dell(conf-ipv6-acl)#
```


Policy-based Routing (PBR)

Policy-based routing (PBR) allows you to apply routing policies to specific interfaces. To enable PBR, create a redirect list and apply it to the interface. After the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list. PBR is supported by the Dell Networking Operating System (OS).

You can apply PBR to physical interfaces and logical interfaces (such as a link aggregation group [LAG] or virtual local area network [VLAN]). Trace lists and redirect lists do not function correctly when you configure both in the same configuration.

 **NOTE:** Apply PBR to Layer 3 interfaces only.

description

Add a description to this redirect list.

Z9500

Syntax	<code>description {description}</code>	
	To remove the description, use the <code>no description {description}</code> command.	
Parameters	<i>description</i>	Enter a description to identify the IP redirect list (80 characters maximum).
Defaults	none	
Command Modes	REDIRECT-LIST	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
	8.4.2.1	Introduced on the C-Series and S-Series.
	8.4.2.0	Introduced on the E-Series TeraScale.
	7.7.1.0	Introduced on the E-Series ExaScale.

ip redirect-group

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

Z9500

Syntax

```
ip redirect-group redirect-list-name
```

To remove a redirect list from an interface, use the `no ip redirect-group name` command.

Parameters

redirect-list-name

Enter the name of a configured redirect list.

Defaults

none

Command Modes

INTERFACE (conf-if-vl-)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.4.2.0	Added support for LAG and VLAN interfaces.
7.7.1.0	Introduced on the E-Series ExaScale.

Usage Information

You can apply any number of redirect-groups to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.

If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise, the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.



NOTE: Apply the redirect list to physical, VLAN, or LAG interfaces only.

**Related
Commands**

- [show cam pbr](#) – displays the content of the PBR CAM.
- [show ip redirect-list](#) – displays the redirect-list configuration.

ip redirect-list

Configure a redirect list and enter REDIRECT-LIST mode.

Z9500

Syntax

```
ip redirect-list redirect-list-name
```

To remove a redirect list, use the `no ip redirect-list` command.

Parameters

redirect-list-name

Enter the name of a redirect list.

Defaults

none

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
6.5.3.0	Introduced on the E-Series ExaScale.

permit

Configure a rule for the redirect list.

Z9500

Syntax

```
permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]
```

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq sequence-number syntax` command.
- You can also use the `no permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]` command.

Parameters	<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
	<i>protocol-type</i>	Enter one of the following keywords as the protocol type: • <code>icmp</code> for internet control message protocol • <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
	<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
	<i>mask</i>	Enter a network mask in /prefix format (/x).
	<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
	<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
	<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
	<i>bit</i>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • <code>ack</code> = acknowledgement • <code>fin</code> = finish (no more data from the user) • <code>psh</code> = push function • <code>rst</code> = reset the connection • <code>syn</code> = synchronize sequence number • <code>urg</code> = urgent field

<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>portcommand</code> parameter.)
Defaults	none
Command Modes	REDIRECT-LIST
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.5.1.0	Introduced on the E-Series ExaScale.

redirect

Configure a rule for the redirect list.

Z9500

Syntax	<pre>redirect {ip-address slot/port} {ip-protocol-number protocol-type [bit]} {source mask any host ip-address} {destination mask any host ip-address} [operator]</pre> To remove this filter, use one of the following: • Use the <code>no seq sequence-number</code> command if you know the filter's sequence number. • You can also use the <code>no redirect {ip-address slot/port} {ip-protocol-number [bit] protocol-type} {source mask any host ip-address} {destination mask any host ip-address} [operator]</code> command.
---------------	---

Parameters

<i>ip-address</i>	Enter the IP address of the forwarding router.
<i>slot/port</i>	Enter the keyword <code>slot / port</code> followed by the slot/port information.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: • <code>icmp</code> for internet control message protocol • <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
<i>bit</i>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • <code>ack</code> = acknowledgement • <code>fin</code> = finish (no more data from the user) • <code>psh</code> = push function • <code>rst</code> = reset the connection • <code>syn</code> = synchronize sequence number • <code>urg</code> = urgent field
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	Enter a network mask in /prefix format (/x).
<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command parameter.)

Defaults

none

Command Modes

REDIRECT-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series.
8.4.2.0	Introduced on the E-Series TeraScale.

seq

Configure a filter with an assigned sequence number for the redirect list.

Z9500

Syntax

```
seq sequence-number {permit | redirect {ip-address}} {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operator]{source-port source-port| source-port-range start-port - end-port} {destination-port destination-port| destination-port-range start-port - end-port}
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

<i>sequence-number</i>	Enter a number from 1 to 65535.
<i>permit</i>	Enter the keyword <code>permit</code> assign the sequence to the permit list.
<i>redirect</i>	Enter the keyword <code>redirect</code> to assign the sequence to the redirect list.
<i>ip-address</i>	Enter the IP address of the forwarding router.
<i>ip-protocol-number</i>	Enter the keyword <code>ip-protocol-number</code> then the number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: <code>icmp</code> for internet control message protocol

	• <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	Enter a network mask in /prefix format (/x).
<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>bit</i>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • <code>ack</code> = acknowledgement • <code>fin</code> = finish (no more data from the user) • <code>psh</code> = push function • <code>rst</code> = reset the connection • <code>syn</code> = synchronize sequence number • <code>urg</code> = urgent field
<i>operator</i>	(OPTIONAL) For the TCP and UDP parameters only. Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the port command parameter.)
<i>source port</i>	Enter the keywords <code>source-port</code> then the port number to be matched in the ACL rule in the ICAP rule
<i>destination-port</i>	Enter the keywords <code>destination-port</code> then the port number to be matched in the ACL rule in the ICAP rule.
<i>source-port-range</i>	Enter the keywords <code>Source-port-range</code> then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.
<i>destination-port-range</i>	Enter the keywords <code>destination-port-range</code> then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.

Defaults	none						
Command Modes	REDIRECT-LIST						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.4(0.0)</td><td>Introduced on the S4810, S4820T, S6000, and Z9000.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.						

show cam pbr

Display the PBR CAM content.

Z9500

Syntax	<pre>show cam pbr {[interface <i>interface</i>] linecard <i>slot-number</i> port-set <i>number</i>]} [summary]</pre>									
Parameters	<table><tr><td>interface <i>interface</i></td><td>Enter the keyword <code>interface</code> then the name of the interface.</td></tr><tr><td>linecard <i>number</i></td><td>Enter the keyword <code>linecard</code> then the slot number. The range is from 0 to 2 .</td></tr><tr><td>port-set <i>number</i></td><td>Enter the keywords <code>port-set</code> then the port-pipe number. The port-pipe number is from 0 to 3.</td></tr><tr><td>summary</td><td>Enter the keyword <code>summary</code> to view only the total number of CAM entries.</td></tr></table>	interface <i>interface</i>	Enter the keyword <code>interface</code> then the name of the interface.	linecard <i>number</i>	Enter the keyword <code>linecard</code> then the slot number. The range is from 0 to 2 .	port-set <i>number</i>	Enter the keywords <code>port-set</code> then the port-pipe number. The port-pipe number is from 0 to 3.	summary	Enter the keyword <code>summary</code> to view only the total number of CAM entries.	
interface <i>interface</i>	Enter the keyword <code>interface</code> then the name of the interface.									
linecard <i>number</i>	Enter the keyword <code>linecard</code> then the slot number. The range is from 0 to 2 .									
port-set <i>number</i>	Enter the keywords <code>port-set</code> then the port-pipe number. The port-pipe number is from 0 to 3.									
summary	Enter the keyword <code>summary</code> to view only the total number of CAM entries.									
Defaults	none									
Command Modes	EXEC									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.				
Version	Description									
9.5(0.1)	Introduced on the Z9500.									

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Example

```
Dell#show ip redirect-list

IP redirect-list ecmp:
Defined as:
seq 5 redirect 100.1.1.1 ip any any, Next-hop reachable (via
Vl 1001), ARP resolved
Vl 1002), ARP resolved
Vl 1003), ARP resolved
Vl 1004), ARP resolved
Vl 1005), ARP resolved
Vl 1006), ARP resolved
Vl 1007), ARP resolved
Vl 1008), ARP resolved
Applied interfaces:
Vl 100
Dell#
```

Port Monitoring

The port monitoring feature allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

Important Points to Remember

- Port monitoring is supported on physical ports and logical interfaces, such as port channels and virtual local area networks (VLANs).
- The monitoring (destination, “MG”) and monitored (source, “MD”) ports must be on the same switch.
- In general, a monitoring port should have `no ip address` and `no shutdown` as the only configuration; Dell Networking OS permits a limited set of commands for monitoring ports; display them using the `?` command. A monitoring port also may not be a member of a VLAN.
- A total of 4 MG may be configured in a single port-pipe.
- MG and MD ports can be reside anywhere across a port-pipe.
- The Dell Networking OS supports multiple source ports to be monitored by a single destination port in one monitor session.
- One monitor session can have only one MG port.

 **NOTE:** The monitoring port should not be a part of any other configuration.

description

Enter a description of this monitoring session.

Z9500

Syntax	<code>description {description}</code>	
	To remove the description, use the <code>no description {description}</code> command.	
Parameters	description	Enter a description regarding this session (80 characters maximum).
Defaults	none	
Command Modes	CONFIGURATION	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.7.1.0	Introduced on the E-Series.

Related Commands

[monitor session](#) — enables a monitoring session.

monitor session

Create a session for monitoring traffic with port monitoring.

Z9500

Syntax

```
monitor session session-ID (type { rpm | erpm })
```

To delete a session, use the `no monitor session session-ID` command.

To delete all monitor sessions, use the `no monitor session all` command.

Parameters

<i>session-ID</i>	Enter a session identification number. The range is from 0 to 65535.
type rpm erpm	Specifies one of the following type: - rpm: to create remote port monitoring session. - erpm: to create encapsulated remote port monitoring session.

Defaults

none

Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.4(0.0)</td><td>Introduced on the S4810, S4820T, S6000, and Z9000.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the MXL.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.	9.0.2.0	Introduced on the S6000.	9.0.2.0	Introduced on the MXL.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description														
9.5(0.1)	Introduced on the Z9500.														
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.														
9.0.2.0	Introduced on the S6000.														
9.0.2.0	Introduced on the MXL.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
Usage Information	The <code>monitor</code> command is saved in the running configuration at Monitor Session mode level and can be restored after a chassis reload.														
Example	<pre>Dell(config)# monitor session 60 Dell(config-mon-sess-60)</pre>														
Related Command	show monitor session — displays the monitor session. show running-config monitor session — displays the running configuration of a monitor session.														

show config

Display the current monitor session configuration.

Z9500

Syntax	<code>show config</code>
Defaults	none
Command Modes	MONITOR SESSION (conf-mon-sess-session-ID)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell(conf-mon-sess-2)#show config
!
monitor session 2 type rpm
  source fortyGigE 0/60 destination remote-vlan 300 direction rx
  source Port-channel 10 destination remote-vlan 300 direction
  rx
  no disable
Dell#
```

show monitor session

Display information about monitoring sessions.

Z9500

Syntax

```
show monitor session {session-ID}
```

To display monitoring information for all sessions, use the `show monitor session` command.

Parameters

session-ID (OPTIONAL) Enter a session identification number. The range is from 0 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4.0.0	Added support for the RPM / ERPM.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show monitor session
SessID  Source      Destination      Dir      Mode      Source IP
Dest IP
-----  -
1      Te 0/1      Te 0/4          both     Port      N/
A      N/A
2      Po 128      remote-vlan 100  tx       Port      N/
A      N/A
3      Te 0/2      remote-ip       rx       Port      36.36.36.1
72.72.72.2
```

Related Commands

[monitor session](#) — creates a monitoring session.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

Z9500

Syntax

```
show running-config monitor session {session-ID}
```

To display the running configuration for all monitor sessions, use the `show running-config monitor session` command.

Parameters

session-ID (OPTIONAL) Enter a session identification number. The range from 0 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

The `monitoring` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Example

```
Dell(conf-mon-sess-0)#do show running-config monitor session
!
monitor session 0
  source Port-channel 10 destination TenGigabitEthernet 0/33
direction tx
!
```

Related Commands

[monitor session](#) — creates a monitoring session.

[show monitor session](#) — displays a monitoring session.

source (port monitoring)

Configure a port monitor source.

Z9500

Syntax

```
source interface | range destination interface direction {rx | tx | both}
```

To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

Parameters

source interface	Enter the one of the following keywords and slot/port information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface enter the keyword <code>VLAN</code> followed by a number from 1 to 4094. - For a port channel interface, enter the keyword <code>port-channel</code> followed by the port-channel id .
range	Enter the keyword <code>range</code> to specify the list of interfaces.
destination	Enter the keyword <code>destination</code> to specify the destination interface. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keyword <code>port-channel</code> followed by the port-channel id .
interface	Enter the one of the following keywords and slot/port information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface enter the keyword <code>VLAN</code> followed by a number from 1 to 4094. - For a port channel interface, enter the keyword <code>port-channel</code> followed by the port-channel id .
direction {rx tx both}	Enter the keyword <code>direction</code> then one of the packet directional indicators. <code>rx</code>: to monitor receiving packets only. <code>tx</code>: to monitor transmitting packets only. <code>both</code>: to monitor both transmitting and receiving packets.

Defaults

none

**Command
Modes**

MONITOR SESSION (conf-mon- sess-session-ID)

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4.0.0	Added support for Source and destination.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell# monitor session 0
source Port-channel 10 destination TenGigabitEthernet 0/33
direction tx
```

Private VLAN (PVLAN)

The private VLAN (PVLAN) feature of the Dell Networking operating software.

Private VLANs extend the system security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair. The private VLAN implementation is based on RFC 3069.

For more information, refer to the following commands. The command output is augmented in the Dell Networking OS version 7.8.1.0 at later to provide PVLAN data:

- [show arp](#)
- [show vlan](#)

Private VLAN Concepts

Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice versa.

Port Types:

- *Community port:* A community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.

- *Isolated port*: An isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- *Promiscuous port*: A promiscuous port is a port that is allowed to communicate with any other port type.
- *Trunk port*: A trunk port carries VLAN traffic across switches:
 - A trunk port in a PVLAN is always tagged.
 - A trunk port in Tagged mode carries primary or secondary VLAN traffic. The tag on the packet helps identify the VLAN to which the packet belongs.
 - A trunk port can also belong to a regular VLAN (non-private VLAN).

ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

Z9500

Syntax

```
[no] ip local-proxy-arp
```

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the primary VLAN.

To disable Layer 3 communication in a particular secondary VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the selected secondary VLAN.



NOTE: Even after you disable `ip-local-proxy-arp` (use `no ip-local-proxy-arp`) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the address resolution protocol (ARP) timeout happens on those secondary VLAN hosts.

Defaults

Layer 3 communication is disabled between secondary VLANs in a private VLAN.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	7.8.1.0	Introduced on the C-Series and S-Series.
Version	Description				
7.8.1.0	Introduced on the C-Series and S-Series.				
Related Commands	private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary. private-vlan mapping secondary-vlan — maps secondary VLANs to the selected primary VLAN. show arp — displays the ARP table. show interfaces private-vlan — displays the type and status of the PVLAN interfaces. show vlan private-vlan — displays the PVLANS and/or interfaces that are part of a PVLAN. switchport mode private-vlan — sets PVLAN mode of the selected port.				

private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

Z9500

Syntax	<pre>[no] private-vlan mode {community isolated primary}</pre> To remove the PVLAN configuration, use the <code>no private-vlan mode {community isolated primary}</code> command syntax.	
Parameters	community	Enter the keyword <code>community</code> to set the VLAN as a community VLAN.
	isolated	Enter the keyword <code>isolated</code> to configure the VLAN as an isolated VLAN.
	primary	Enter the keyword <code>primary</code> to configure the VLAN as a primary VLAN.
Defaults	none	
Command Modes	INTERFACE VLAN	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

The VLAN:

- can be in only one mode, either `community`, `isolated`, or `primary`.
- mode ode to `community` or `isolated` even before associating it to a primary VLAN. This secondary VLAN continues to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message indicates this.)
- must not have a port in it when VLAN mode is being set.

Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as previously described) can be added to the PVLAN. No other regular ports can be added to the PVLAN.

After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

Related Commands

[private-vlan mapping secondary-vlan](#) — maps secondary VLANs to the selected primary VLAN.

[show interfaces private-vlan](#) — displays the type and status of the PVLAN interfaces.

[show vlan private-vlan](#) — displays the PVLANS and/or interfaces that are part of a PVLAN.

[switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

Z9500

Syntax

```
[no] private-vlan mapping secondary-vlan vlan-list
```

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` command syntax.

Parameters	<i>vlan-list</i> Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.												
Defaults	none												
Command Modes	INTERFACE VLAN												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the C-Series and S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
7.8.1.0	Introduced on the C-Series and S-Series.												
Usage Information	The list of secondary VLANs can be: - Specified in comma-delimited or hyphenated-range format. - Specified with this command even before they have been created. - Amended by specifying the new secondary VLAN to be added to the list.												
Related Commands	private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary. show interfaces private-vlan — displays the type and status of the PVLAN interfaces. show vlan private-vlan — displays the PVLANS and/or interfaces that are part of a PVLAN. switchport mode private-vlan — sets PVLAN mode of the selected port.												

show interfaces private-vlan

Display type and status of PVLAN interfaces.

Z9500

Syntax	show interfaces private-vlan [interface <i>interface</i>]	
Parameters	interface <i>interface</i>	(OPTIONAL) Enter the keyword <i>interface</i> followed by the interface type and slot/port numbers or port-channel number to specify the port(s) for which you want to display PVLAN information. The range of Z9500 slot IDs is 0 to 2. Enter only a slot ID to display the PVLAN status for all ports on a Z9500 line card. The valid values are: • port-channel <i>port-channel-number</i> • tengigabitethernet [<i>slot-id</i> <i>slot/port</i>] • fortygigE [<i>slot-id</i> <i>slot/port</i>]

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

The following describes the `show interfaces private-vlan` command shown in the Examples below.

Field	Description
Interface	Displays the type of interface and associated slot and port number.

Field	Description
Vlan	Displays the VLAN ID of the designated interface.
PVLAN-Type	Displays the type of VLAN in which the designated interface resides.
Interface Type	Displays the PVLAN port type of the designated interface.
Status	States whether the interface is operationally up or down.

Example (All)

```
Dell# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
-----
Fo 1/52 30 Isolated Host Up
Fo 2/12 20 Community Host Up
Po 10 10 Primary Trunk Up
```

Example (Specific)

```
Dell# show interfaces private-vlan te 2/2
Interface Vlan PVLAN-Type Interface Type Status
-----
Te 2/2 100 Isolated Host Up
```

Related Commands

[private-vlan mode](#) – sets the mode of the selected VLAN to community, isolated, or primary.

[show vlan private-vlan](#) – displays the PVLANS and/or interfaces that are part of a PVLAN.

[switchport mode private-vlan](#) – sets PVLAN mode of the selected port.

show vlan private-vlan

Display PVLAN configurations, including member interfaces, type, and status.

Z9500

Syntax

```
show vlan private-vlan [vlan-id | community vlan-id | interface
interface | isolated vlan-id | mapping vlan-id | primary vlan-id]
```

Parameters

<i>vlan-id</i>	(OPTIONAL) Enter a VLAN ID number to display the PVLAN configuration.
community <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>community</code> and a PVLAN ID number to display the configuration for a community PVLAN.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> followed by the interface type and slot/port numbers or port-channel number to display the PVLAN configuration for a member

	interface. The range of Z9500 slot IDs is 0 to 2. The valid values are:												
	• port-channel <i>port-channel-number</i> • tengigabitethernet <i>slot/port</i> • fortygigE <i>slot/port</i>												
	isolated (OPTIONAL) Enter the keyword <code>isolated</code> and a PVLAN ID number to display the configuration of an isolated PVLAN. mapping (OPTIONAL) Enter the keyword <code>mapping</code> to display the community and isolated PVLAN mapping to primary PVLANS. primary vlan-id (OPTIONAL) Enter the keyword <code>primary</code> and a PVLAN ID number to display the configuration of a primary PVLAN.												
Defaults	none												
Command Modes	• EXEC • EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.1</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.1	Introduced on the S4810.	7.8.1.0	Introduced on the C-Series and S-Series.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.1	Introduced on the S4810.												
7.8.1.0	Introduced on the C-Series and S-Series.												
Usage Information	Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANS and their member VLANs and interfaces. The other types of output show details about PVLAN subsets. The following describes the <code>show private-vlan</code> command shown in the Examples below. <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Primary</td><td>Displays the VLAN ID of the designated or associated primary VLAN(s).</td></tr> <tr> <td>Secondary</td><td>Displays the VLAN ID of the designated or associated secondary VLAN(s).</td></tr> </table>	Field	Description	Primary	Displays the VLAN ID of the designated or associated primary VLAN(s).	Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s).						
Field	Description												
Primary	Displays the VLAN ID of the designated or associated primary VLAN(s).												
Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s).												

Field	Description
Type	Displays the type of VLAN in which the listed interfaces reside.
Active	States whether the interface is operationally up or down.
Ports	Displays the interface IDs in the listed VLAN.

Example (All)

```
Dell# show vlan private-vlan
Primary Secondary Type      Active Ports
-----
10          100      primary  Yes    Te 2/1,3
           101      isolated Yes    Te 2/2
           101      community Yes    Te 2/10
20          200      primary  Yes    Po 10, 12-13
           200      isolated Yes    Te 1/1
           201      community No     Te 1/2,4-6
           202      community Yes    Te 1/11-12
```

Example (Primary)

```
Dell# show vlan private-vlan primary
Primary Secondary Type      Active Ports
-----
10          primary  Yes    Te 2/1,3
20          primary  Yes    Te 1/1,3
```

Example (Isolated)

```
Dell# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
-----
10          100      primary  Yes    Te 2/1,3
           100      isolated Yes    Te 2/2,4-6
           200      isolated Yes    Te 1/2,4-6
```

Example (Community)

```
Dell# show vlan private-vlan community
Primary Secondary Type      Active Ports
-----
10          101      primary  Yes    Te 2/1,3
           101      community Yes    Te 2/7-10
20          201      primary  Yes    Po 10, 12-13
           201      community No     Te 1/1
           202      community Yes    Te 1/11-12
```

Example (Interface)

```
Dell# show vlan private-vlan interface te 2/1
Primary Secondary Type      Active Ports
-----
10          primary  Yes    Te 2/1
```

Example (Mapping)

```
Dell# show vlan private-vlan mapping

Private Vlan:
  Primary   : 10
  Isolated  : 30
  Community : 20
```

Usage Information

Note that if the VLAN ID you enter is a primary VLAN, the entire private VLAN output is displayed, as shown below. If the VLAN ID is a secondary VLAN, only its primary VLAN and secondary VLAN properties are displayed, as shown in the second Example below.

Example

```
Dell# show vlan private-vlan 10
Primary Secondary Type      Active  Ports
-----
10              primary  Yes    Te 2/1,3
              102      isolated Yes    Te 0/4
              101      community Yes    Te 2/7-10
```

Example

```
Dell#show vlan private-vlan 102
Primary Secondary Type      Active  Ports
-----
10              Primary  Yes    Po 1
              Te 0/2
              102      Isolated Yes    Te 0/4
```

Related Commands

[private-vlan mode](#) – sets the mode of the selected VLAN to community, isolated, or primary.

[show interfaces private-vlan](#) – displays type and status of PVLAN interfaces.

[switchport mode private-vlan](#) – sets PVLAN mode of the selected port.

switchport mode private-vlan

Set PVLAN mode of the selected port.

Z9500

Syntax

```
[no] switchport mode private-vlan {host | promiscuous | trunk}
To remove PVLAN mode from the selected port, use the no switchport mode private-vlan command.
```

Parameters

host	Enter the keyword <code>host</code> to configure the selected port or port channel as an isolated interface in a PVLAN.
promiscuous	Enter the keyword <code>promiscuous</code> to configure the selected port or port channel as an promiscuous interface.
trunk	Enter the keyword <code>trunk</code> to configure the selected port or port channel as a trunk port in a PVLAN.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown in the following example.

Example

```
Dell#conf
Dell(conf)#interface TenGigabitEthernet 2/1
Dell(conf-if-te-2/1)#switchport mode private-vlan promiscuous

Dell(conf)#interface TenGigabitEthernet 2/2
Dell(conf-if-te-2/2)#switchport mode private-vlan host

Dell(conf)#interface TenGigabitEthernet 2/3
Dell(conf-if-te-2/3)#switchport mode private-vlan trunk

Dell(conf)#interface port-channel 10
Dell(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

Related Commands

[private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.

[private-vlan mapping secondary-vlan](#) — sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it.

[show interfaces private-vlan](#) — displays type and status of PVLAN interfaces.

Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking operating software implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1w standard spanning tree protocol.

 **NOTE:** For easier command line entry, the plus (+) sign is not used at the command line.

description

Enter a description of the PVST+.

Z9500

Syntax	<code>description {description}</code> To remove the description, use the <code>no description {description}</code> command.													
Parameters	description	Enter a description to identify the spanning tree (80 characters maximum).												
Defaults	none													
Command Modes	SPANNING TREE PVST+ (The prompt is "config-pvst".)													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.1</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.1	Introduced.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.7.1.1	Introduced.													
Related Commands	protocol spanning-tree pvst — enter SPANNING TREE mode on the switch.													

disable

Disable PVST+ globally.

Z9500

Syntax	<code>disable</code> To enable PVST+, use the <code>no disable</code> command.																
Defaults	Disabled.																
Command Modes	CONFIGURATION (conf-pvst)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Related Commands	protocol spanning-tree pvst — enter PVST+ mode.																

extend system-id

To augment the Bridge ID with a VLAN ID so that PVST+ differentiate between BPDUs for each VLAN, use extend system ID. If the VLAN receives a BPDU meant for another VLAN, PVST+ does not detect a loop, and both ports can remain in Forwarding state.

Z9500

Syntax	<code>extend system-id</code>
Defaults	Disabled
Command Modes	PROTOCOL PVST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

Example

```
Dell(conf-pvst)#do show spanning-tree pvst vlan 5 brief
VLAN 5
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32773, Address 0001.e832.73f7
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32773 (priority 32768 sys-id-ext 5),
Address 0001.e832.73f7
We are the root of Vlan 5
Configured hello time 2, max age 20, forward delay 15

Interface Designated
Name      PortID  Prio  Cost  Sts Cost Bridge ID      PortID
-----
Te 0/10 128.140 128  200000 FWD 0   32773 0001.e832.73f7
128.140
Te 0/12 128.142 128  200000 DIS 0   32773 0001.e832.73f7
128.142

Interface
Name      Role PortID  Prio  Cost  Sts Cost Link-type Edge
-----
Te 0/10  Desg 128.140 128  200000 FWD 0   P2P      No
Te 0/12  Dis  128.142 128  200000 DIS 0   P2P      No
```

Related Commands

[protocol spanning-tree pvst](#) – enter SPANNING TREE mode on the switch.

protocol spanning-tree pvst

To enable PVST+ on a device, enter the PVST+ mode.

Z9500

Syntax

```
protocol spanning-tree pvst
```

To disable PVST+, use the `disable` command.

Defaults	none																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>8.3.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	8.3.1.0	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
8.3.1.0	Introduced.																
Example	<pre> Dell#conf Dell(conf)#protocol spanning-tree pvst Dell(conf-pvst)#no disable Dell(conf-pvst)#vlan 2 bridge-priority 4096 Dell(conf-pvst)#vlan 3 bridge-priority 16384 Dell(conf-pvst)# Dell(conf-pvst)#show config ! protocol spanning-tree pvst no disable vlan 2 bridge-priority 4096 vlan 3 bridge-priority 16384 Dell# </pre>																
Usage Information	After you enable PVST+, the device runs an STP instance for each VLAN it supports.																
Related Commands	disable — disables PVST+. show spanning-tree pvst — displays the PVST+ configuration.																

show spanning-tree pvst

View the Per-VLAN spanning tree configuration.

Z9500

Syntax	show spanning-tree pvst [vlan vlan-id] [brief] [guard]	
Parameters	vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID. The range is 1 to 4094.
	brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the PVST+ configuration information.
	interface	(OPTIONAL) Enter one of the interface keywords along with the slot/port information: - For a Port Channel interface, enter the keyword <code>port-channel</code> then a number: The range is 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	guard	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on a PVST interface and the current port state.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

Version	Description
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency and Port VLAN ID inconsistency.
6.2.1.1	Introduced.

Usage Information

The following describes the `show spanning-tree pvst` command shown in the following examples.

Field	Description
Interface Name	PVST interface.
Instance	PVST instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Brief)

```
Dell#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4096, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface                               Designated
Name      PortID  Prio Cost Sts Cost  Bridge ID  PortID
-----
Te 1/0    128.130 128 20000 FWD 20000 4096 0001.e801.6aa8
128.426
Te 1/1    128.131 128 20000 BLK 20000 4096 0001.e801.6aa8
128.427
Te 1/16   128.146 128 20000 FWD 20000 16384 0001.e805.e306
128.146
Te 1/17   128.147 128 20000 FWD 20000 16384 0001.e805.e306
128.147

Interface
Name      Role PortID  Prio Cost  Sts Cost Link-type Edge
-----
Te 1/0    Root 128.130 128 20000 FWD 20000 P2P      No
Te 1/1    Altr 128.131 128 20000 BLK 20000 P2P      No
Te 1/16   Desg 128.146 128 20000 FWD 20000 P2P      Yes
Te 1/17   Desg 128.147 128 20000 FWD 20000 P2P      Yes
```

Example

```
Dell#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
```

```

Number of topology changes 3, last change occurred 00:57:00

Port 130 (TenGigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.130
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (TenGigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 0
The port is not in the Edge port mode

Port 146 (TenGigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1578, received 0
The port is in the Edge port mode

Port 147 (TenGigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier
128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode

```

**Example (EDS/
LBK)**

```

Dell#show spanning-tree pvst vlan 2 interface
tengigabitethernet 1/0

```

TenGigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding

```

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

```

```

Interface Designated
Name      PortID   Prio Cost   Sts Cost Bridge ID      PortID
-----
Te 1/0    128.1223 128   20000 EDS 0 32768 0001.e800.a12b 128.1223

```

**Example (EDS/
PVID)**

```

Dell#show spanning-tree pvst vlan 2 interface
tengigabitethernet 1/0

```

TenGigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

```
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 1, received 0
```

```
Interface Designated
Name      PortID    Prio Cost    Sts Cost Bridge ID          PortID
-----
Te 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (Guard)

```
Dell#show spanning-tree pvst vlan 5 guard
Interface
Name      Instance Sts          Guard type
-----
Te 0/1 5          INCON(Root) Rootguard
Te 0/2 5          FWD         Loopguard
Te 0/3 5          EDS(Shut)   Bpduguard
```

Related Commands

[spanning-tree pvst](#) — configure PVST+ on an interface.

spanning-tree pvst

Configure a PVST+ interface with one of these settings: edge port with optional bridge port data unit (BPDU) guard, port disablement if an error condition occurs, port priority or cost for a VLAN range, loop guard, or root guard.

Z9500

Syntax

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-
violation]] | err-disable | vlan vlan-range {cost number |
priority value} | loopguard | rootguard}
```

Parameters

edge-port	Enter the keywords <code>edge-port</code> to configure the interface as a PVST+ edge port.
bpduguard	Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
err-disable	Enter the keywords <code>err-disable</code> to enable the port to be put into the error-disable state (EDS) if an error condition occurs.

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
cost <i>number</i>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. Defaults: 10-Gigabit Ethernet interface = 2000. - Port Channel interface with one 10 Gigabit Ethernet = 2000. - Port Channel with two 10 Gigabit Ethernet = 1800.
priority <i>value</i>	Enter the keyword <code>priority</code> then the Port priority value in increments of 16. The range is from 0 to 240. The default is 128 .
loopguard	Enter the keyword <code>loopguard</code> to enable loop guard on a PVST+ port or port-channel interface.
rootguard	Enter the keyword <code>rootguard</code> to enable root guard on a PVST+ port or port-channel interface.
Defaults	Not configured.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Introduced the <code>loopguard</code> and <code>rootguard</code> options on the E-Series TeraScale, C-Series, and S-Series.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the hardware <code>shutdown-on-violation</code> option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the optional Bridge Port Data Unit (BPDU) guard.
6.2.1.1	Introduced.

Usage Information

The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into the Error Disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.



NOTE: A port configured as an edge port, on a PVST switch, immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the route process module (RPM) CPU.

You cannot enable `root guard` and `loop guard` at the same time on a port. For example, if you configure `loop guard` on a port on which `root guard` is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard.`

When used in a PVST+ network, loop guard is performed per-port or per-port channel at a VLAN level. If no BPDUs are received on a VLAN interface, the port or port-channel transitions to a Loop-Inconsistent (blocking) state only for this VLAN.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
Dell(conf-if-te-1/1)#spanning-tree pvst vlan 3 cost 18000
Dell(conf-if-te-1/1)#end
Dell(conf-if-te-1/1)#show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-te-1/1)#end
```

Related Commands

[show spanning-tree pvst](#) — views the PVST+ configuration.

spanning-tree pvst err-disable

Place ports in an Err-Disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

Z9500

Syntax	<code>spanning-tree pvst err-disable cause invalid-pvst-bpdu</code>												
Defaults	Enabled; ports are placed in the Err-Disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.												
Command Modes	INTERFACE												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced.
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
8.2.1.0	Introduced.												
Usage Information	Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU. Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, the system places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent the system from executing this action, use the <code>no spanning-tree pvst err-disable</code> command cause <code>invalid-pvst-bpdu</code>.												
Related Commands	show spanning-tree pvst — views the PVST+ configuration.												

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Z9500

Syntax	<code>tc-flush-standard</code>
---------------	--------------------------------

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information

By default, the system implements an optimized flush mechanism for PVST+. This implementation helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this *knob* command on to enable flushing MAC addresses after receiving every topology change notification.

vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

Z9500

Syntax

`vlan vlan-range bridge-priority value`

To return to the default value, use the `no vlan bridge-priority` command.

Parameters

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
bridge-priority <i>value</i>	Enter the keywords <code>bridge-priority</code> then the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is 32768 .

Defaults	32768																
Command Modes	CONFIGURATION (conf-pvst)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced.																
Related Commands	vlan forward-delay — changes the time interval before the system transitions to the Forwarding state. vlan hello-time — change the time interval between BPDUs. vlan max-age — changes the time interval before PVST+ refreshes. show spanning-tree pvst — displays the PVST+ configuration.																

vlan forward-delay

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

Z9500

Syntax	<pre>vlan <i>vlan-range</i> forward-delay <i>seconds</i></pre> To return to the default setting, use the <code>no vlan forward-delay</code> command.	
Parameters	vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
	forward-delay <i>seconds</i>	Enter the keywords <code>forward-delay</code> then the time interval, in seconds, that the system waits before transitioning PVST+

to the forwarding state. The range is from 4 to 30 seconds.
The default is **15 seconds**.

Defaults **15 seconds**

Command Modes CONFIGURATION (conf-pvst)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands

- [vlan bridge-priority](#) — sets the bridge-priority value.
- [vlan hello-time](#) — changes the time interval between BPDUs.
- [vlan max-age](#) — changes the time interval before PVST+ refreshes.
- [show spanning-tree pvst](#) — displays the PVST+ configuration.

vlan hello-time

Set the time interval between generation of PVST+ 7 BPDUs.

Z9500

Syntax `vlan vlan-range hello-time seconds`
To return to the default value, use the `no vlan hello-time` command.

Parameters

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
-------------------------------	---

	hello-time seconds	Enter the keywords <code>hello-time</code> then the time interval, in seconds, between transmission of BPDUs. The range is from 1 to 10 seconds. The default is 2 seconds .																
Defaults	2 seconds																	
Command Modes	CONFIGURATION (conf-pvst)																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced.																	
Related Commands	vlan bridge-priority — sets the bridge-priority value. vlan forward-delay — changes the time interval before the system transitions to the forwarding state. vlan max-age — changes the time interval before PVST+ refreshes. show spanning-tree pvst — displays the PVST+ configuration.																	

vlan max-age

To maintain configuration information before refreshing that information, set the time interval for the PVST+ bridge.

Z9500

Syntax	<code>vlan <i>vlan-range</i> max-age <i>seconds</i></code> To return to the default, use the <code>no vlan max-age</code> command.	
Parameters	vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.

	max-age seconds Enter the keywords <code>max-age</code> then the time interval, in seconds, that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is 20 seconds.																
Defaults	20 seconds																
Command Modes	CONFIGURATION (conf-pvst)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced.																
Related Commands	vlan bridge-priority — sets the bridge-priority value. vlan forward-delay — changes the time interval before the system transitions to the forwarding state. vlan hello-time — changes the time interval between BPDUs. show spanning-tree pvst — displays the PVST+ configuration.																

Quality of Service (QoS)

The Dell Networking operating software commands for quality of service (QoS) include traffic conditioning and congestion control.

This chapter contains the following sections:

- [Global Configuration Commands](#)
- [Per-Port QoS Commands](#)
- [Policy-Based QoS Commands](#)

Global Configuration Commands

There is only one global configuration QoS command.

qos-rate-adjust

Enable QoS rate adjustment to include overhead fields in rate metering calculations.

Z9500

Syntax	<code>qos-rate-adjust overhead-bytes-number</code>	
Parameters	<i>overhead-bytes-number</i>	Enter the number of bytes of packet overhead to include in rate limiting, policing, and shaping calculations. The range is from 1 to 31.
Defaults	QoS rate adjustment is disabled by default.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>8.3.1.0</td><td>Introduced.</td></tr> </table>	Version	Description	8.3.1.0	Introduced.
Version	Description				
8.3.1.0	Introduced.				
Usage Information	By default, when rate policing and shaping, the system does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations.				

service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

Z9500

Syntax	<code>service-class bandwidth-percentage queue0 <i>percentage</i> queue1 <i>percentage</i> queue2 <i>percentage</i> queue3 <i>percentage</i></code>													
Parameters	<i>percentage</i>	Enter the bandwidth-weight as a percentage. The range is from 1 to 100.												
Defaults	none													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.1</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.1	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series and S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.1	Introduced on the S4810.													
8.2.1.0	Introduced on the C-Series and S-Series.													
Usage Information	Guarantee a minimum bandwidth to different queues globally using the <code>service-class bandwidth-percentage</code> command from CONFIGURATION mode. The command is applied in the same way as the <code>bandwidth-percentage</code> command in an output QoS policy. The <code>bandwidth-percentage</code> command in QOS-POLICY-OUT mode supersedes the <code>service-class bandwidth-percentage</code> command.													

service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

Z9500

Syntax	service-class dot1p-mapping {dot1p0 value dot1p1 value dot1p2 value dot1p3 value dot1p4 value dot1p5 value dot1p6 value dot1p7 value}													
Parameters	dot1p0 value ... dot1p7 value	Enter a dot1p list number and value. The list number range is from 0 to 7. The range is from 0 to 3.												
Defaults	For each dot1p Priority, the default CoS queue value is: - dot1p Priority: 0 1 2 3 4 5 6 7 - CoS Queue: 2 0 1 3 4 5 6 7													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.16.0</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.													
Usage Information	To apply dot1p-queue-mapping, use the service-class dynamic dot1p command.													
Related Commands	show qos dot1p-queue-mapping — displays the dot1p priority to queue mapping on the switch.													

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes an INTERFACE mode entry.

Z9500

Syntax `service-class dynamic dot1p`

To return to the default setting, use the `no service-class dynamic dot1p` command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

dot1p	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Command Modes

- INTERFACE
- CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the <code>kbps</code> option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded the command to permit configuration on port channels.
6.1.1.1	Introduced on the E-Series.

Usage Information

To honor all incoming 802.1p markings on incoming switched traffic on the interface, enter this command. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

You can apply this command on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the `service-class dynamic` command to individual interfaces in a port channel.

- All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command on an interface or globally.
- Layer 2 or Layer 3 service policies supersede dot1p service classes.

service-class wred backplane

After you create a WRED profile with ECN functionality, specify per-queue granularity for backplane ports and include the WRED profile in a service class. Using this command, you can enable or disable queue-specific settings and specify minimum and maximum buffer thresholds in the WRED profile applied to each packet color-code. Also, you can specify the maximum drop rate percentage for yellow and green profiles. The per-queue profile configured is applied to all the backplane ports.

Z9500

Syntax

```
[no] service-class wred {green | weight | yellow} {[queue0
number/string] || [queue1 number/string] || [queue2 number/
string] || [queue3 number/string] || [queue4 number/string] ||
[queue5 number/string] || [queue6 number/string] || [queue7
number/string]} backplane
```

Parameters

service-class	Define the mapping between the service class and policy-based QoS or routing.
wred	Specify WRED curve parameters for a queue
green	Specify green (low) drop precedence to a queue.
weight	Specify a weight factor to a queue.
yellow	Specify yellow (medium) drop precedence to a queue.
queue 0 to queue 7	Specify the queue number to which the WRED parameters apply.
number	Enter a weight for the queue as a number in the range of 1 to 15. This parameter applies only if you specify the green or yellow drop precedence.
string	Enter the WRED profile name. It is a string of up to 32 characters. Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_. This parameter applies only if you specify a weight factor.
backplane	Specify that the WRED weight and profile configured for each queue apply to backplane ports.

Default

All queues on backplane ports operate in tail-drop (best-effort traffic) mode by default. There is no default WRED green or yellow profile. The default weight is 0.

Command Modes	QOS-POLICY-OUT mode	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the Z9000 platform.
Usage Information	You can configure all the data queues. For Z9500, you can configure queues 0-3. WRED profile contains a set of characteristics, such as the minimum and maximum WRED thresholds and the maximum drop rate. You can add and remove WRED parameters for one or more queues by using the command in a single line. All of the configured attributes apply to all the backplane ports and are for each queue. To assign drop precedence to green or yellow traffic, use this command. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.	
Example	<pre>Dell(conf-wred)#wred thresh-1 Dell(conf-wred)#threshold min 100 max 200 max-drop-rate 40 Dell(conf-wred)#wred thresh-2 Dell(conf-wred)#threshold min 300 max 400 max-drop-rate 80 Dell(conf)#service-class wred green queue5 thresh-1 queue7 thresh-2 backplane Dell(conf)#service-class wred yellow queue1 thresh-2 queue3 thresh-1 backplane Dell(conf)#service-class wred weight queue0 11 queue6 4 queue7 9 backplane</pre>	

service-class wred ecn backplane

Apply ECN marking on backplane port-queues in a service class.

Z9500

Syntax	<code>[no] service-class wred ecn <i>queue-list</i> backplane</code>	
Parameters	service-class	Define the mapping between the service class and policy-based QoS or routing.
	wred	Associate WRED with ECN to mark packets instead of dropping them.
	ecn	Cause explicit congestion notification (ECN) to be used to indicate network congestion, rather than dropping packets, <i>queues-list</i> Enter the queue numbers, either as individual queue numbers separated by commas or as an inclusive list separating the starting and ending queue numbers with a hyphen
	<i>queue-list</i>	Enter the port-queue numbers, either as individual queue numbers separated by commas or as an inclusive list separating the starting and ending queue numbers with a hyphen; for example, <code>service-class wred ecn 0, 2, 4-6 backplane</code> . The range of queue IDs is 0 to 7.

	backplane	Specify that the ECN marking configured for each queue applies to backplane ports.	
Default	By default, ECN marking is disabled on all queues.		
Command Modes	CONFIGURATION mode		
Command History	Version	Description	
	9.3.0.0	Introduced on the Z9500 switch.	
	9.3.0.0	Introduced on the Z9000 platform.	
Usage Information	You can add or remove ECN marking configuration on a list of queues on all backplane ports. All of the configured attributes apply to all the backplane ports and are for each queue. You can configure all the data queues. For the Z9500, you can configure queues 0-7. By default, ECN marking is disabled on all queues. When you enable WRED with ECN and the number of packets in the queue is below the minimum threshold, packets are transmitted per the usual WRED treatment. When you enable WRED with ECN and the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following three scenarios can occur: • If the transmission endpoints are ECN-capable and traffic is congested, and the WRED algorithm determines that the packet should be dropped based on the drop probability, the packet is transmitted and marked so the routers know the system is congested and can slow transmission rates. • If neither endpoint is ECN-capable, the packet may be dropped based on the WRED drop probability. This behavior is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router. • If the network is experiencing congestion, the packet is transmitted. No further marking is required. When you enable WRED with ECN and the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This behavior is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.		

Example `Dell(conf)#service-class wred ecn 0, 3-5, 7 backplane`

service-pool wred

Configure a global buffer pool that serves as a shared buffer accessed by multiple queues when the minimum guaranteed buffers for a queue are consumed.

The Z9500 supports four global service-pools in the egress direction. Two service pools are used—one for lossy queues and the other for lossless (priority-based flow control (PFC)) queues. You can enable WRED and ECN operation on the global service-pools. You can define WRED profiles and weight on each of the global service-pools for both lossy and lossless (PFC) service-pools.

Z9500

Syntax	<code>[no] buffer-pool wred {green weight yellow} {[pool0 number/string] [pool1 number/string]}</code>	
Parameters	buffer-pool	Define the mapping between the service class and policy-based QoS or routing.
	wred	Specify WRED curve parameters for a queue.
	green	Specify green (low) drop precedence to a queue.
	weight	Specify a weight factor to a queue
	yellow	Specify yellow (medium) drop precedence to a queue
	pool0	Service-pool buffer 1 (default service-pool for PFC traffic)
	pool1	Service-pool buffer 0 (default service-pool for lossy traffic)
	number	Enter a weight for the queue as a number in the range of 1 to 15. This parameter applies only if you specify the green or yellow drop precedence.
	string	Enter the WRED profile name. It is a string of up to 32 characters. Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred_ge_y, wred_ge_g, wred_teng_y, wred_teng_. This parameter applies only if you specify a weight factor.
Default	All queues on backplane ports operate in tail-drop (best-effort traffic) mode by default. There is no default WRED green or yellow profile. The default weight is 0.	
Command Modes	CONFIGURATION mode	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the S6000 and Z9000 platforms.
Usage Information	You can configure only service pools 0 and 1 because the Dell Networking OS uses only these two service pools. The service0 pool is used for lossy queues; the service1 pool is used for lossless (PFC) queues on all platforms. You can configure the weight for the WRED average queue size on service1 pool on which PFC is supported; service0 pool does not support PFC. A WRED profile contains a set of attributes, such as the minimum and maximum threshold values, and the maximum drop rate for the received packets. You can add or remove WRED parameter configurations for one or more shared service pools using a single command. The <code>buffer-pool wred</code> command is similar in usage and working to the <code>service-class bandwidth-percentage queue-id</code> command.	

Example

```
Dell(conf-wred)#wred thresh-1
Dell(conf-wred)#threshold min 100 max 200 max-drop-rate 40

Dell(conf-wred)#wred thresh-2
Dell(conf-wred)#threshold min 300 max 400 max-drop-rate 80

Dell(conf)#service-pool wred green pool0 thresh-1 pool1
thresh-2
Dell(conf)#service-pool wred yellow pool0 thresh-3 pool1
thresh-4
Dell(conf)#service-pool wred weight pool0 11 pool1 4
```

show qos dot1p-queue-mapping

Displays the dot1p priority to queue mapping on the switch.

Z9500

Syntax

```
show qos dot1p-queue-mapping
```

Defaults

- dot1p Priority: 0 1 2 3 4 5 6 7
- Queue: 0 0 0 1 2 3 3 3

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on MXL 10/40GbE Switch IO Module.

Related Commands

[service-class dot1p-mapping](#) — Identifies the class map.

Per-Port QoS Commands

Per-port QoS (port-based QoS) allows you to define the QoS configuration on a per-physical-port basis.

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic this interface receives.

Z9500

Syntax dot1p-priority *priority-value*
To delete the IEEE 802.1p configuration on the interface, use the no dot1p-priority command.

Parameters	<i>priority-value</i>	Enter a value from 0 to 7.	
	dot1p	Queue Number	
	0	2	
	1	0	
	2	1	
	3	3	
	4	4	
	5	5	
	6	6	
	7	7	

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the `dot1p-priority` command to individual interfaces in a port channel.

rate police

Police the incoming traffic rate on the selected interface.

Z9500

Syntax

```
rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

Parameters

kbps	Enter the keyword <code>kbps</code> to specify the rate limit in Kilobits per second (Kbps).
committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is 50 .
peak peak-rate	(OPTIONAL) Enter the keyword <code>peak</code> then a number to specify the peak rate in Mbps. The range is from 0 to 40000.
vlan vlan-id	(OPTIONAL) Enter the keyword <code>vlan</code> then a VLAN ID to police traffic to those specific VLANs. The range is from 1 to 4094.

Defaults

Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Added the <code>kbps</code> option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information



NOTE: Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface. For each physical interface, you can configure three `rate police` commands specifying different VLANs.

Related Commands

[rate-police](#) — specifies traffic policing on the selected interface.

rate shape

Shape the traffic output on the selected interface.

Z9500

Syntax

```
rate shape [kbps] rate [burst-KB]
```

Parameters

kbps	(Optional) Enter the keyword <code>kbps</code> to specify the rate limit in kilobits per second (Kbps). The range is from 0 to 10000000. The default granularity is Megabits per second (Mbps).
rate	Enter the outgoing rate in multiples of 10 Mbps. The range is from 0 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is 50.

Defaults

Granularity for rate is **Mbps** unless you use the `kbps` option.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the <code>kbps</code> option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series and C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information If traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured.

Related Commands [rate-shape](#) — shapes traffic output as part of the designated policy.

strict-priority

Configure a unicast queue as a strict-priority (SP) queue.

Z9500

Syntax	<code>strict-priority unicast queue-number</code>	
Parameters	unicast <i>queue-number</i>	Enter the keyword <code>unicast</code> with the number for a strict-priority queue. The range of queue numbers is from 1 to 7.
Defaults	none	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

	Version	Description
	6.1.1.1	Introduced on the E-Series.
Usage Information	After you configure a unicast queue as strict-priority, the specified queue is treated as a strict-priority queue on the entire switch. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over a strict-priority queue, it starves all other queues on the ports on which this traffic is flowing.	

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes. The system allows you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

Z9500

Syntax	<code>bandwidth-percentage percentage</code> To remove the bandwidth percentage, use the <code>no bandwidth-percentage</code> command.	
Parameters	<i>percentage</i>	Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).
Defaults	none	
Command Modes	CONFIGURATION (conf-qos-policy-out)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.1.9.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	6.2.1.1	Introduced on the E-Series.
Version	Description				
6.2.1.1	Introduced on the E-Series.				
Usage Information	The unit of bandwidth percentage is 1%. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage automatically scales down to 100%.				
Related Commands	qos-policy-output — creates a QoS output policy.				

class-map

Create a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

Z9500

Syntax	<code>class-map {match-all match-any} class-map-name [layer2] [cpu-qos]</code>					
Parameters	match-all	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords <code>match-all</code> to determine that the packets must meet all the match criteria in order to be a member of the class.				
	match-any	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords <code>match-any</code> to determine that the packets must meet at least one of the match criteria in order to be a member of the class.				
	class-map-name	Enter a name of the class for the class map in a character format (32 character maximum).				
	layer2	Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .				
	cpu-qos	Enter the keyword <code>cpu-qos</code> to create a class map to filter protocol traffic for rate-limiting control-plane traffic (CoPP).				
Defaults	Layer 3					
Command Modes	CONFIGURATION					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Class-map names can be 32 characters. Layer2 available on the C-Series and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Expanded to add support for Layer 2.

Usage Information

Packets arriving at the input interface are checked against the match criteria and configured using this command to determine if the packet belongs to that class. This command accesses CLASS-MAP mode, where the configuration commands include `match ip` and `match mac` options.

When you create a class map to filter protocol traffic for CoPP, you must enter the keyword `cpu-qos`.

Related Commands

[ip access-list extended](#) — configures an extended IP ACL.

[ip access-list standard](#) — configures a standard IP ACL.

[match ip access-group](#) — configures the match criteria based on the access control list (ACL).

[match ip precedence](#) — identifies the IP precedence values as match criteria.

[match ip dscp](#) — configures the match criteria based on the DSCP value.

[match mac access-group](#) — configures a match criterion for a class map based on the contents of the designated MAC ACL.

[match mac dot1p](#) — configures a match criterion for a class map based on a dot1p value.

[match mac vlan](#) — configures a match criterion for a class map based on VLAN ID.

[service-queue](#) — assigns a class map and QoS policy to different queues.

[show qos class-map](#) — views the current class map information.

clear qos statistics

Clears Matched Packets through class maps applied to inbound ports

Z9500

Syntax	<code>clear qos statistics interface-name</code>																	
Parameters	<i>interface-name</i>	Enter one of the following keywords: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.																
Defaults	none																	
Command Modes	• EXEC • EXEC Privilege																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.18.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.18.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.18.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.1	Introduced on the E-Series.																	
Related Commands	show qos statistics — displays the QoS statistics.																	

description

Add a description to the selected policy map or QoS policy.

Z9500

Syntax	<code>description {description}</code>
--------	--

To remove the description, use the `no description {description}` command.

Parameters	<i>description</i>	Enter a description to identify the policies (80 characters maximum).										
Defaults	none											
Command Modes	CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><td>Version 9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>Version 8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>Version 8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>Version 8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>pre-Version 7.7.1.0</td><td>Introduced.</td></tr></table>		Version 9.2(1.0)	Introduced on the Z9500.	Version 8.3.19.0	Introduced on the S4820T.	Version 8.3.11.1	Introduced on the Z9000.	Version 8.3.7.0	Introduced on the S4810.	pre-Version 7.7.1.0	Introduced.
Version 9.2(1.0)	Introduced on the Z9500.											
Version 8.3.19.0	Introduced on the S4820T.											
Version 8.3.11.1	Introduced on the Z9000.											
Version 8.3.7.0	Introduced on the S4810.											
pre-Version 7.7.1.0	Introduced.											
Related Commands	policy-map-input — creates an input policy map. policy-map-output — creates an output policy map. qos-policy-input — creates an input QoS-policy on the router. qos-policy-output — creates an output QoS-policy on the router. wred-profile — creates a WRED profile.											

match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

Z9500

Syntax	<code>match ip access-group access-group-name [set-ip-dscp value]</code> To remove ACL match criteria from a class map, use the <code>no match ip access-group access-group-name [set-ip-dscp value]</code> command.	
Parameters	<i>access-group-name</i>	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the class-map specifies.

	set-ip-dscp value	(OPTIONAL) Enter the keywords <code>set-ip-dscp</code> then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.																						
Defaults	none																							
Command Modes	CLASS-MAP CONFIGURATION (config-class-map)																							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.0</td><td>Added the <code>DSCP Marking</code> option support on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.5.1.0</td><td>Added support for the <code>DSCP Marking</code> option.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Added the <code>DSCP Marking</code> option support on the S-Series.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	7.5.1.0	Added support for the <code>DSCP Marking</code> option.	6.1.1.1	Introduced on the E-Series.
Version	Description																							
9.2(1.0)	Introduced on the Z9500.																							
8.3.19.0	Introduced on the S4820T.																							
8.3.11.1	Introduced on the Z9000.																							
8.3.11.1	Introduced on the Z9000.																							
8.3.7.0	Introduced on the S4810.																							
7.7.1.0	Added the <code>DSCP Marking</code> option support on the S-Series.																							
7.6.1.0	Introduced on the S-Series.																							
7.5.1.0	Introduced on the C-Series.																							
7.5.1.0	Added support for the <code>DSCP Marking</code> option.																							
6.1.1.1	Introduced on the E-Series.																							
Usage Information	To access this command, enter the <code>class-map</code> command. After the class map is identified, you can configure the match criteria. For <code>class-map match-any</code>, a maximum of five ACL match criteria are allowed. For <code>class-map match-all</code>, only one ACL match criteria is allowed.																							
Related Commands	class-map — identifies the class map.																							

match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.

Z9500

Syntax	<pre>match {ip ipv6 ip-any} dscp dscp-list [set-ip-dscp value]</pre> To remove a DSCP value as a match criteria, use the <code>no match {ip ipv6 ip-any} dscp dscp-list [[multicast] set-ip-dscp value]</code> command.	
Parameters	ip	Enter the keyword <code>ip</code> to support IPv4 traffic.

ipv6	Enter the keyword <code>ipv6</code> to support IPv6 traffic.
ip-any	Enter the keyword <code>ip-any</code> to support IPv4 and IPv6 traffic.
dscp-list	Enter the IP DSCP values that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 63.
set-ip-dscp value	(OPTIONAL) Enter the keywords <code>set-ip-dscp</code> then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults none

Command Modes CLASS-MAP CONFIGURATION (`config-class-map`)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added the ipv6 and ip-any options on the Z9500.
9.5(0.0)	Added the ipv6 and ip-any options on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the keyword <code>multicast</code> . Added the DSCP Marking option support on the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series. Added support for the DSCP Marking option.
6.2.1.1	Introduced on the E-Series.

Usage Information To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip dscp` and `match ip precedence` commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DSCP values 0 1 2 3 4 5 6 7, enter either the `match ip dscp 0,1,2,3,4,5,6,7` or `match ip dscp 0-7` command.



NOTE: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values must match.

Related Commands [class-map](#) — identifies the class map.

match ip precedence

Use IP precedence values as a match criteria.

Z9500

Syntax

```
match {ip | ipv6 | ip-any} precedence ip-precedence-list [set-  
ip-dscp value]
```

To remove IP precedence as a match criteria, use the `no match {ip | ipv6 | ip-any} precedence ip-precedence-list [[multicast] set-ip-dscp value]` command.

Parameters

ip	Enter the keyword <code>ip</code> to support IPv4 traffic.
ipv6	Enter the keyword <code>ipv6</code> to support IPv6 traffic.
ip-any	Enter the keyword <code>ip-any</code> to support IPv4 and IPv6 traffic.
ip- precedence-list	Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 7.
set-ip-dscp value	(OPTIONAL) Enter the keywords <code>set-ip-dscp</code> then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (`config-class-map`)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for the ipv6 and ip-any options on the Z9500.

Version	Description
9.5(0.0)	Added support for the ipv6 and ip-any options on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the keyword <code>multicast</code> . Added support for the <code>DSCP marking</code> option for the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.5.1.0	Added support for the <code>DSCP Marking</code> option.
6.1.1.1	Introduced on the E-Series.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip precedence` command and the `match ip dscp` command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3, enter either the `match ip precedence 0-3` or `match ip precedence 0,1,2,3` command.



NOTE: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values must match.

Related Commands

[class-map](#) — identifies the class map.

match ip vlan

Uses a VLAN as the match criterion for an L3 class map.

Z9500

Syntax

```
match ip vlan vlan-id
```

To remove VLAN as the match criterion, use the `no match ip vlan vlan-id` command.

Parameters	vlan <i>vlan-id</i>	Enter the keyword <code>vlan</code> and then the ID of the VLAN. The range is from 1 to 4094.						
Defaults	none							
Command Modes	CONF-CLASS-MAP							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.4.(0.0)</td><td>Introduced on the S-Series and Z-Series.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.4.(0.0)	Introduced on the S-Series and Z-Series.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
9.4.(0.0)	Introduced on the S-Series and Z-Series.							
Usage Information	To access this command, enter the <code>class-map</code> command. After the class map is identified, you can configure the match criteria. Use this command to match an IP class-map against a single VLAN ID .							
Related Commands	class-map — identifies the class map.							

match mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

Z9500

Syntax	<code>match mac access-group {mac-acl-name}</code>							
Parameters	mac-acl-name	Enter a MAC ACL name. Its contents is used as the match criteria in the class map.						
Defaults	none							
Command Modes	CLASS-MAP							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Available on the C-Series and S-Series.
	7.5.1.0	Added support for the DSCP <i>Marking</i> option.
	7.4.1.0	Introduced.
Usage Information	To access this command, enter the <code>class-map</code> command. After the class map is identified, you can configure the match criteria.	
Related Commands	class-map — identifies the class map.	

match mac dot1p

Configure a match criterion for a class map based on a dot1p value.

Z9500

Syntax	<code>match mac dot1p {dot1p-list}</code>	
Parameters	dot1p-list	Enter a dot1p value. The range is from 0 to 7.
Defaults	none	
Command Modes	CLASS-MAP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Available on the C-Series and S-Series.
	7.5.1.0	Added support for the DSCP <i>Marking</i> option.
	7.4.1.0	Introduced.
Usage Information	To access this command, enter the <code>class-map</code> command. After the class map is identified, you can configure the match criteria.	

Related [class-map](#) — identifies the class map.
Commands

match mac vlan

Configure a match criterion for a class map based on VLAN ID.

Z9500

Syntax `match mac vlan number`

Parameters *number* Enter the VLAN ID. The range is from 1 to 4094.

Defaults none

Command Modes CLASS-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced.

Usage Information To access this command, enter the `class-map` command. You can match against only one VLAN ID.

Related [class-map](#) — identifies the class map.
Commands

policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

Z9500

Syntax `policy-aggregate qos-policy-name`
To remove a policy aggregate configuration, use the `no policy-aggregate qos-policy-name` command.

Parameters	<i>qos-policy-name</i>	Enter the name of the policy map in character format (32 characters maximum).																		
Defaults	none																			
Command Modes	CONFIGURATION (policy-map-input and policy-map-output)																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Policy name character limit increased from 16 to 32.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Policy name character limit increased from 16 to 32.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
8.2.1.0	Policy name character limit increased from 16 to 32.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			
Usage Information	An aggregate output QoS policy applies to all outbound port traffic. An aggregate output QoS policy can coexist with per-queue output QoS policies.																			
Related Commands	policy-map-input — creates an input policy map. policy-map-output — creates an output policy map.																			

policy-map-input

Create an input policy map.

Z9500

Syntax	<pre>policy-map-input <i>policy-map-name</i> [layer2] [cpu-qos]</pre> To remove an input policy map, use the <code>no policy-map-input <i>policy-map-name</i> [layer2] [cpu-qos]</code> command.	
Parameters	<i>policy-map-name</i>	Enter the name of the policy map in character format (32 characters maximum).
	layer2	(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .

	cpu-qos	(OPTIONAL) Enter the keyword <code>cpu-qos</code> to create an input policy to be used to rate-limit control-plane traffic (CoPP).																				
Defaults	Layer 3																					
Command Modes	CONFIGURATION																					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Policy name character limit increased from 16 to 32.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Expanded to add support for Layer 2.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Policy name character limit increased from 16 to 32.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	7.4.1.0	Expanded to add support for Layer 2.	6.1.1.1	Introduced on the E-Series.
Version	Description																					
9.2(1.0)	Introduced on the Z9500.																					
8.3.19.0	Introduced on the S4820T.																					
8.3.11.1	Introduced on the Z9000.																					
8.3.7.0	Introduced on the S4810.																					
8.2.1.0	Policy name character limit increased from 16 to 32.																					
7.6.1.0	Introduced on the S-Series.																					
7.5.1.0	Introduced on the C-Series.																					
7.4.1.0	Expanded to add support for Layer 2.																					
6.1.1.1	Introduced on the E-Series.																					
Usage Information	The input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or incoming packets DSCP. This command enables Policy-Map-Input Configuration mode (conf-policy-map-in). When you configure an input policy map for CoPP, you must enter the keyword <code>cpu-qos</code>.																					
Related Commands	service-queue — assigns a class map and QoS policy to different queues. policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps. service-policy input — applies an input policy map to the selected interface.																					

policy-map-output

Create an output policy map.

Z9500

Syntax `policy-map-output policy-map-name`

To remove a policy map, use the `no policy-map-output policy-map-name` command.

Parameters

policy-map-name Enter the name for the policy map in character format (32 characters maximum).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (conf-policy-map-out).

Related Commands

[service-queue](#) — assigns a class map and QoS policy to different queues.

[policy-aggregate](#) — allows an aggregate method of configuring per-port QoS using policy maps.

[service-policy output](#) — applies an output policy map to the selected interface.

qos-policy-input

Create a QoS input policy on the router.

Z9500

Syntax

`qos-policy-input qos-policy-name [layer2] [cpu-qos]`

To remove an existing input QoS policy from the router, use the `no qos-policy-input qos-policy-name [layer2] [cpu-qos]` command.

Parameters	qos-policy-name	Enter the name for the policy map in character format (32 characters maximum).																		
	layer2	(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .																		
	cpu-qos	Enter the keyword <code>cpu-qos</code> to create a QoS input policy to be used to rate-limit control-plane traffic (CoPP).																		
Defaults	Layer 3																			
Command Modes	CONFIGURATION																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Policy name character limit increased from 16 to 32.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Policy name character limit increased from 16 to 32.	7.6.1.0	Introduced on the C-Series and S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
8.2.1.0	Policy name character limit increased from 16 to 32.																			
7.6.1.0	Introduced on the C-Series and S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.1.1.1	Introduced on the E-Series.																			
Usage Information	To specify the name of the input QoS policy, use this command. After the input policy is specified, <code>rate-police</code> is defined. This command enables Qos-Policy-Input Configuration mode — (<code>conf-qos-policy-in</code>). When changing a Service-Queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the <code>show qos statistics</code> command is reset. If you create create a QoS input policy to be used for CoPP, you must enter the keyword <code>cpu-qos</code>.																			
	Related Commands																			
	rate police — incoming traffic policing function.																			

qos-policy-output

Create a QoS output policy.

Z9500

Syntax `qos-policy-output qos-policy-name`
To remove an existing output QoS policy, use the `no qos-policy-output qos-policy-name` command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (32 characters maximum).
------------------------	--

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information To specify the name of the output QoS policy, use this command. After the output policy is specified, rate-shape, bandwidth-percentage, and WRED can be defined. This command enables Qos-Policy-Output Configuration mode — (conf-qos-policy-out).

Related Commands

- [rate shape](#) — rate-shape traffic functionality.
- [bandwidth-percentage](#) — assigns weight to the class/queue percentage.
- [wred](#) — assigns yellow or green drop precedence.

rate-police

Specify the policing functionality on incoming traffic.

Z9500

Syntax `rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]`

Parameters	kbps	Enter the keyword <code>kbps</code> to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
	committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 40000.
	burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is 100 .
	peak peak-rate	(OPTIONAL) Enter the keyword <code>peak</code> then a number to specify the peak rate in Mbps. The range is from 0 to 40000. The default is the same as designated for <code>committed-rate</code> .

Defaults Burst size is 100KB. `peak-rate` is by default the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

Command Modes QOS-POLICY-IN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the <code>kbps</code> option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information	The default burst size is 100Kb. If a different value is required, you must configure the burst size to the required value.
Related Commands	rate shape — shapes traffic output as part of the designated policy. qos-policy-input — creates a QoS output policy.

rate-shape

Shape traffic output as part of an output QoS policy.

Z9500

Syntax	<pre>rate-shape {kbps pps} peak-rate {burst-kbps burst-packets} [committed {kbps pps} committed-rate {burst-kbps burst- packets}]</pre>	
Parameters	kbps	Enter the keyword <code>kbps</code> to specify the rate limit in kilobits per second (Kbps). The range is from 0 to 40000000.
	pps	Enter the keyword <code>pps</code> to specify the rate limit in packets per second (pps). The range is from .
	<i>burst-kbps</i>	Enter the peak rate or committed rate size in kilobits per second. The range is from . The default is .
	<i>burst-packets</i>	Enter the peak rate or committed rate size in packets per second. The range is from . The default is .
Defaults		
Command Modes	QOS-POLICY-OUT	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description						
7.5.1.0	Introduced on the C-Series.						
6.1.1.1	Introduced on the E-Series.						
Usage Information	You must configure the peak rate and peak burst size using the same value: kilobits or packets per second. Similarly, you must configure the committed rate and committed burst size with the same measurement. Peak rate refers to the maximum rate for traffic arriving or exiting an interface under normal traffic conditions. Peak burst size indicates the maximum size of unused peak bandwidth that is aggregated. This aggregated bandwidth enables brief durations of burst traffic that exceeds the peak rate and committed burst. Committed rate refers to the guaranteed bandwidth for traffic entering or leaving the interface under normal network conditions. When traffic propagates at an average rate that is less than or equal to the committed rate, it is considered to be green-colored or coded. When the transmitted traffic falls below the committed rate, the bandwidth, which is not used by any traffic that is traversing the network, is aggregated to form the committed burst size. Traffic is considered to be green-colored up to the point at which the unused bandwidth does not exceed the committed burst size.						
Related Commands	qos-policy-output — creates a QoS output policy. rate police — specifies traffic policing on the selected interface.						

service-policy input

Apply an input policy map to the selected interface.

Z9500

Syntax	<pre>service-policy input <i>policy-map-name</i> [layer2]</pre> To remove the input policy map from the interface, use the <code>no service-policy input <i>policy-map-name</i> [layer2]</code> command.				
Parameters	<table> <tr> <td><i>policy-map-name</i></td><td>Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.</td></tr> <tr> <td><i>layer2</i></td><td>(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3.</td></tr> </table>	<i>policy-map-name</i>	Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.	<i>layer2</i>	(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .
<i>policy-map-name</i>	Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.				
<i>layer2</i>	(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .				
Defaults	Layer 3				
Command Modes	INTERFACE				

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Expanded to add support for Layer 2.
6.1.1.1	Introduced on the E-Series.

Usage Information

You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.



NOTE: The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface. However, the `service-policy input` command (without the `policy-map-name` option) and the `service-class dynamic dot1p` command are allowed on an interface.

Related Commands

[policy-map-input](#) — creates an input policy map.

service-policy output

Apply an output policy map to the selected interface.

Z9500

Syntax

```
service-policy output policy-map-name
```

To remove the output policy map from the interface, use the `no service-policy output policy-map-name` command.

Parameters

policy-map-name

Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults

none

Command Modes	INTERFACE														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the C-Series and S-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the C-Series and S-Series.														
6.1.1.1	Introduced on the E-Series.														
Usage Information	A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.														
Related Commands	policy-map-output — creates an output policy map.														

service-queue

Assign a class map and QoS policy to different queues.

Z9500

Syntax	<pre>service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]</pre> To remove the queue assignment, use the <code>no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]</code> command.	
Parameters	queue-id	Enter the value used to identify a queue. The range is from 0 to 7 (eight data queues and eight control queues).
	class-map class-map-name	(OPTIONAL) Enter the keyword <code>class-map</code> then the class map name assigned to the queue in character format (32 character maximum).
	qos-policy qos-policy-name	(OPTIONAL) Enter the keywords <code>qos-policy</code> then the QoS policy name assigned to the queue in text format (32 characters maximum). This specifies the input QoS policy



NOTE: This option is available under `policy-map-input` only.

assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

Defaults	none																
Command Modes	CONFIGURATION (conf-policy-map-in and conf-policy-map-out)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.1.1.1	Introduced on the E-Series.																
Usage Information	There are eight queues per interface on the Z9500. This command assigns a class map or QoS policy to different queues.																
Related Commands	class-map — identifies the class map. service-policy input — applies an input policy map to the selected interface. service-policy output — applies an output policy map to the selected interface.																

set

Mark outgoing traffic with a differentiated service code point (DSCP) or dot1p value.

Z9500

Syntax	<code>set {ip-dscp value mac-dot1p value}</code>	
Parameters	ip-dscp value	(OPTIONAL) Enter the keywords <code>ip-dscp</code> then the IP DSCP value. The range is from 0 to 63.
	mac-dot1p value	Enter the keywords <code>mac-dot1p</code> then the dot1p value. The range is from 0 to 7.
Defaults	none	

Command Modes	CONFIGURATION (conf-qos-policy-in)																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Added <code>mac-dot1p</code> on the C-Series and S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>E-Series Only: Added support for <code>mac-dot1p</code>.</td></tr> <tr> <td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Added <code>mac-dot1p</code> on the C-Series and S-Series.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	7.4.1.0	E-Series Only: Added support for <code>mac-dot1p</code> .	6.1.1.1	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.2.1.0	Added <code>mac-dot1p</code> on the C-Series and S-Series.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
7.4.1.0	E-Series Only: Added support for <code>mac-dot1p</code> .																				
6.1.1.1	Introduced on the E-Series.																				
Usage Information	After the IP DSCP bit is set, other QoS services can then operate on the bit settings.																				

show qos class-map

View the current class map information.

Z9500

Syntax	<code>show qos class-map [class-name]</code>				
Parameters	<i>class-name</i> (Optional) Enter the name of a configured class map.				
Defaults	none				
Command Modes	- EXEC - EXEC Privilege				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Related Commands

[class-map](#) — identifies the class map.

show qos policy-map

View the QoS policy map information.

Z9500

Syntax

```
show qos policy-map {summary [interface] | detail [interface]}
```

Parameters

summary ***interface***

To view a policy map interface summary, enter the keyword **summary** and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword **fortyGigE** then the slot/port information.

detail *interface*

To view a policy map interface in detail, enter the keyword **detail** and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword **fortyGigE** then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series only: Added Trust IPv6 diffserv.
6.2.1.1	Introduced on the E-Series.

Example (IPv4)

```
Dell#show qos policy-map detail tengigabitethernet 1/1

Interface TenGigabitEthernet 1/1

Policy-map-input policy
Trust diffserv
Queue# Class-map-name Qos-policy-name
0 - q0
1 CM1q1
2 CM2q2
3 CM3q3
4 CM4q4
5 CM5q5
6 CM6q6
7 CM7q7
Dell#
```

Example (IPv6)

```
Dell# show qos policy-map detail tengigabitethernet 0/10

Interface TengigabitEthernet 0/10

Policy-map-input pmap1
Queue# Class-map-name Qos-policy-name
0      c0      q0
1      c1      q1
2      c2      q2
3      c3      q3
4      c4      q4
5      c5      -
6      c6      q6
7      c7      q7
Dell#
```

Example (Summary IPv4)

```
Dell#sho qos policy-map summary

Interface policy-map-input policy-map-output
Te 2/1      PM1      -
```

show qos policy-map-input

View the input QoS policy map details.

Z9500

Syntax `show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]`

Parameters

<i>policy-map-name</i>	Enter the policy map name.
<i>class class-map-name</i>	Enter the keyword <code>class</code> then the class map name.
<i>qos-policy-input qos-policy-name</i>	Enter the keyword <code>qos-policy-input</code> then the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version 9.2(1.0)	Introduced on the Z9500.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
Version 7.4.1.0	E-Series Only: Added Trust IPv6 diffserv.
pre-Version 6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue# Class-map-name Qos-policy-name
```

```
0      ClassMap1      qosPolicyInput
Dell#
```

Example

```
Dell# show qos policy-map-input

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#   Class-map-name   Qos-policy-name
0        c0                q0
1        c1                q1
2        c2                q2
3        c3                q3
4        c4                q4
5        c5                -
6        c6                q6
7        c7                q7
Dell#
```

show qos policy-map-output

View the output QoS policy map details.

Z9500

Syntax

```
show qos policy-map-output [policy-map-name] [qos-policy-output
qos-policy-name]
```

Parameters

<i>policy-map-name</i>	Enter the policy map name.
<i>qos-policy-output qos-policy-name</i>	Enter the keyword <i>qos-policy-output</i> then the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#    Qos-policy-name
    0      qosPolicyOutput
Dell#
```

show qos qos-policy-input

View the input QoS policy details.

Z9500

Syntax `show qos qos-policy-input [qos-policy-name]`

Parameters

<i>qos-policy-name</i>	Enter the QoS policy name.
-------------------------------	----------------------------

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos qos-policy-input

Qos-policy-input QosInput
    Rate-police 100 50 peak 100 50
```


Dell#

show qos qos-policy-output

View the output QoS policy details.

Z9500

Syntax	<code>show qos qos-policy-output [<i>qos-policy-name</i>]</code>	
Parameters	<i>qos-policy-name</i>	Enter the QoS policy name.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos qos-policy-output
Qos-policy-output qosOut
  Rate-limit 50 50 peak 50 50
  Wred yellow 1
  Wred green 1
```

show qos statistics

View QoS statistics.

Z9500

Syntax `show qos statistics {wred-profile [interface]} | [interface]`

Parameters

wred-profile interface

Enter the keywords `wred-profile` and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

interface

Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.1	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage

Information

Example

```
Dell#show qos statistics te 0/1
```

Queue#	Queued Bytes (Cumulative)	Queued Pkts (Cumulative)	Matched Pkts	Matched Bytes	Dropped Pkts
0	0	0	1883725	1883725000	0
1	0	0	1883725	1883725000	0
2	0	0	1883725	1883725000	0
3	0	0	1883725	1883725000	0
4	0	0	1883725	1883725000	0

```

5      0      0      1883724 1883724000 0
6      0      0      1883720 1883720000 0
7      0      0      1883720 1883720000 0

```

Dell#

Usage Information

The following describes the `show qos statistics` command in the following example.

Field (EF)	Description
Queue #	Queue Number
Queued Bytes	Snapshot of the byte count in that queue.
Queued Pkts	Cumulative packet count in that queue.
Matched Pkts	The number of packets that matched the class-map criteria.
	 NOTE: When you configure <code>trust</code> , matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria.
	 NOTE: When you configure <code>trust</code> , matched byte counters are not incremented in this field.
Dropped Pkts	The total of the number of packets dropped for green, yellow and out-of-profile.

Related Commands

[clear qos statistics](#) — clears counters shown in `show qos statistics`.

show qos wred-profile

View the WRED profile details.

Z9500

Syntax	<code>show qos wred-profile wred-profile-name</code>	
Parameters	wred-profile-name	Enter the WRED profile name to view the profile details.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos wred-profile

Wred-profile-name min-threshold max-threshold
wred_drop          0              0
wred_ge_y          1024           2048
wred_ge_g          2048           4096
wred_teng_y        4096           8192
wred_teng_g        8192           16384
WRED1              2000           7000
```

test cam-usage

Verify CAM usage for an input policy-map configuration.

Z9500

Syntax

```
test cam-usage service-policy input policy-map linecard {slot-id port-set port-pipe| all}
```

Parameters

<i>policy-map</i>	Enter the policy map name.
<i>linecard slot-id</i>	(OPTIONAL) Enter the slot number of a line card and a port-pipe number to verify CAM usage on a specified set of ports. Valid Z9500 slot IDs are 0 to 2. The range of valid port-pipe numbers is: 0 to 2 on line card 0; 0 to 3 on line cards 1 and 2.
<i>port-set port-pipe</i>	
<i>linecard all</i>	(OPTIONAL) Enter the keywords <code>linecard all</code> to verify CAM usage on all line cards.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

This feature allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column contains the size of the CAM space required for the Trust rule and not the Class-map rule.

The following describes the text `cam-usage service-policy input policy-map linecard` command shown in the following example.

Field	Description
Linecard	Indicates the line card slot number.
Portpipe	Indicates the portpipe number.
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules.
	 NOTE: The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, cannot be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface.
	 NOTE: The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a linecard/port-pipe is successful — Allowed (n) — or not successful — Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.



NOTE: In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed; therefore, the output contains only L2ACL CAM partition entries.

Example

```
Dell# test cam-usage service-policy input pmap_l2 linecard all
```

For a L2 Input Policy Map pmap_l2, the output must be as follows,

```
Linecard|Portpipe|CAM Partition|Available CAM|Estimated CAM|
Status                                     |per Port
(Allowed ports)
0 0 L2ACL 500 200
Allowed (2)
0 1 L2ACL 100 200
Exception
1 0 L2ACL 1000 200
Allowed (5)
1 1 L2ACL 0 200
Exception
...
...
...
13 1 L2ACL 400 200
Allowed (2)
Dell#
```

threshold

Specify the minimum and maximum threshold values for the configured WRED profiles.

Z9500

Syntax

```
threshold min number max number
```

To remove the threshold values, use the `no threshold min number max number` command.

Parameters

- min *number*** Enter the keyword `min` then the minimum threshold number for the WRED profile. The range is from 0 to 12000KB.
- max *number*** Enter the keyword `max` then the maximum threshold number for the WRED profile. The range is from 0 to 12000KB.

Defaults

none

Command Modes

CONFIGURATION (config-wred)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

	<table><tr><th>Version</th><th>Description</th></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	8.3.11.1	Introduced on the Z9000.	8.3.8.0	Introduced on the S4810.	6.1.1.1	Introduced on the E-Series.										
Version	Description																		
8.3.11.1	Introduced on the Z9000.																		
8.3.8.0	Introduced on the S4810.																		
6.1.1.1	Introduced on the E-Series.																		
Usage Information	To configure the minimum and maximum threshold values for user-defined profiles, use this command. Additionally, to modify the minimum and maximum threshold values for the pre-defined WRED profiles, use this command. If you delete the threshold values of the pre-defined WRED profiles, the profiles revert to their original default values. <table><tr><th>Pre-Defined WRED Profile Name</th><th>Minimum Threshold</th><th>Maximum Threshold</th></tr><tr><td>wred_drop</td><td>0</td><td>0</td></tr><tr><td>wred_ge_y</td><td>1024</td><td>2048</td></tr><tr><td>wred_ge_g</td><td>2048</td><td>4096</td></tr><tr><td>wred_teng_y</td><td>4096</td><td>8192</td></tr><tr><td>wred_teng_g</td><td>8192</td><td>16384</td></tr></table>	Pre-Defined WRED Profile Name	Minimum Threshold	Maximum Threshold	wred_drop	0	0	wred_ge_y	1024	2048	wred_ge_g	2048	4096	wred_teng_y	4096	8192	wred_teng_g	8192	16384
Pre-Defined WRED Profile Name	Minimum Threshold	Maximum Threshold																	
wred_drop	0	0																	
wred_ge_y	1024	2048																	
wred_ge_g	2048	4096																	
wred_teng_y	4096	8192																	
wred_teng_g	8192	16384																	
Related Commands	wred-profile — creates a WRED profile.																		

trust

Specify dynamic classification (DSCP) or dot1p to trust.

Z9500

Syntax	<code>trust {diffserv [fallback] dot1p [fallback]}</code>						
Parameters	<table> <tr> <td>diffserv</td><td>Enter the keyword <code>diffserv</code> to specify trust of DSCP markings.</td></tr> <tr> <td>dot1p</td><td>Enter the keyword <code>dot1p</code> to specify trust dot1p configuration.</td></tr> <tr> <td>fallback</td><td>Enter the keyword <code>fallback</code> to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.</td></tr> </table>	diffserv	Enter the keyword <code>diffserv</code> to specify trust of DSCP markings.	dot1p	Enter the keyword <code>dot1p</code> to specify trust dot1p configuration.	fallback	Enter the keyword <code>fallback</code> to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.
diffserv	Enter the keyword <code>diffserv</code> to specify trust of DSCP markings.						
dot1p	Enter the keyword <code>dot1p</code> to specify trust dot1p configuration.						
fallback	Enter the keyword <code>fallback</code> to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.						
Defaults	none						
Command Modes	CONFIGURATION (conf-policy-map-in)						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.						

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added <code>fallback</code> to the E-Series.
8.2.1.0	Added <code>dot1p</code> to the C-Series and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added <code>dot1p</code> and <code>IPv6 DSCP</code> .
6.1.1.1	Introduced on the E-Series

Usage Information

When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	Z9500 Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	7	48–63
110XXX		Internetwork Control	6	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	5	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	4	32–47
011XXX	AF3	Flash	3	16–31
010XXX	AF2	Immediate	2	16–31
001XXX	AF1	Priority	1	0–15
000XXX	BE (Best Effort)	Best Effort	0	0–15

wred

Configure a WRED profile for yellow or green traffic.

Z9500

Syntax	<code>wred {yellow green} <i>profile-name</i></code> To remove the WRED drop precedence, use the <code>no wred {yellow green} [<i>profile-name</i>]</code> command.															
Parameters	yellow green	Enter the keyword <code>yellow</code> for yellow traffic. A DSCP value of xxx100, xxx101, and xxx110 maps to yellow. Enter the keyword <code>green</code> for <code>green</code> traffic. A DSCP value of xxx0xx maps to green.														
	<i>profile-name</i>	Enter your WRED profile name in character format (32 character maximum). Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: <code>wred_drop</code> , <code>wred-ge_y</code> , <code>wred_ge_g</code> , <code>wred_teng_y</code> , <code>wred_teng_</code> .														
Defaults	none															
Command Modes	QOS-POLICY-OUT mode															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Profile name character limit increased from 16 to 32.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the .E-Series</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Profile name character limit increased from 16 to 32.	6.1.1.1	Introduced on the .E-Series
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
8.2.1.0	Profile name character limit increased from 16 to 32.															
6.1.1.1	Introduced on the .E-Series															
Usage Information	To assign drop precedence to green or yellow traffic, use this command. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.															
Related Commands	wred-profile — creates a WRED profile and name that profile.															

[trust](#) — defines the dynamic classification to trust DSCP.

wred weight

Configure the weight factor used to determine the average-queue size for WRED and ECN operation. The weight value is used in an output QoS policy applied to a front-end or backplane port.

Z9500

Syntax	<code>[no] wred weight <i>number</i></code>	
Parameters	weight	Define the weight factor to be used for computation of the WRED average-queue size to either enable WRED to discard packets or cause ECN to mark packets that exceed the minimum threshold configured. This setting applies to front-end and backplane ports.
	<i>number</i>	Enter the weight as a number to be used to calculate the average-queue size. The range is 1 to 15. The default is 0.
Default	The default weight is zero.	
Command Modes	QOS-POLICY-OUT mode	
Command History	Version	Description
	9.2.1.0	Introduced on the Z9500 switch.
	9.3.0.0	Introduced on the S6000 and Z9000 platforms
Usage Information	If the average queue size is more than the maximum threshold of WRED, the packet is dropped. If the average queue size is between the minimum and maximum threshold values, the decision to drop or queue the packet is taken based on the packet drop probability. The probability that a packet is dropped depends on the minimum threshold, maximum threshold, and mark probability denominator.	
Example	<code>Dell(conf-qos-policy-out)# wred weight 5</code>	

wred ecn

To indicate network congestion without dropping packets, use explicit congestion notification (ECN).

Z9500

Syntax	<code>wred ecn</code>
	To stop marking packets, use the <code>no wred ecn</code> command.
Defaults	none

Command Modes QOS-POLICY-OUT mode

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820t.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information When you enable `wred ecn`, and the number of packets in the queue is below the minimum threshold, packets are transmitted per the usual WRED treatment.

When you enable `wred ecn`, and the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following scenarios can occur:

- If the transmission endpoints are ECN-capable and traffic is congested, and the WRED algorithm determines that the packet should have been dropped based on the drop probability, the packet is transmitted and marked so the routers know the system is congested and can slow transmission rates.
- If neither endpoint is ECN-capable, the packet may be dropped based on the WRED drop probability. This behavior is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.

When you enable `wred ecn`, and the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This behavior is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Related Commands [wred-profile](#) — creates a WRED profile and name that profile.

wred-profile

Create a WRED profile and name the profile.

Z9500

Syntax `wred-profile wred-profile-name`
To remove an existing WRED profile, use the `no wred-profile` command.

Parameters

<i>wred-profile-name</i>	Enter your WRED profile name in character format (32 character maximum). Or use one of the pre-defined WRED
---------------------------------	---

profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles.

Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

Defaults	The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined wred_ge_g values.												
Command Modes	CONFIGURATION												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>6.1.1.1</td><td>Introduced on the E-Series</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	6.1.1.1	Introduced on the E-Series
Version	Description												
9.2(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.11.1	Introduced on the Z9000.												
8.3.7.0	Introduced on the S4810.												
6.1.1.1	Introduced on the E-Series												
Usage Information	Use the default pre-defined profiles or configure your own profile. You cannot delete the pre-defined profiles or their default values. This command enables WRED configuration mode —(conf-wred).												
Related Commands	threshold — specifies the minimum and maximum threshold values of the WRED profile.												

DSCP Color Map Commands

The DSCP color map allows you to set the number of specific DSCP values to yellow or red. Traffic marked as yellow delivers traffic to the egress queue which will either transmit the packet if it has available bandwidth or drop the packet due to no ability to send. Traffic marked as red (high drop precedence) is dropped.

dscp

Sets the number of specific DSCP values for a color map profile to yellow or red.

Syntax	dscp {yellow red} [<i>list-dscp-values</i>]
--------	---

To remove a color policy map profile, use the `no dscp {yellow | red} [dscp-list]` command.

Parameters

Yellow	Enter the <code>yellow</code> keyword. Traffic marked as yellow delivers traffic to the egress queue which either transmits the packet if it has available bandwidth or drops the packet due to no ability to send.
red	Enter the <code>red</code> keyword. Traffic marked as red is dropped.
dscp-list	Enter a list of IP DSCP values. The <code>dscp-list</code> parameter specifies the full list of IP DSCP value(s) for the specified color. Each DSCP value in a list is separate values by commas – no spaces (1,2,3) or indicates a list of values separated by a hyphen (1-3). Range is 0 to 63.

Defaults

None

Command Modes

CONFIG-COLOR-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

The default setting for each DSCP value (0-63) is green (low drop precedence). This command allows setting the number of specific DSCP values to yellow or red.

Important Points to Remember

- All DSCP values that are not specified as yellow or red are colored green.
- A DSCP value cannot be in both the yellow and red lists. Setting the red or yellow list with any DSCP value that is already in the other list results in an error and no update to that list is made.
- Each color map can only have one list of DSCP values for each color; any DSCP values previously listed for that color that are not in the new DSCP list are colored green.

Example

```
Dell(conf-dscp-color-map)# dscp yellow 9,10,11,13,15,16
```

Related
Commands

[qos dscp-color-map](#) — configures the DSCP color map

[qos dscp-color-policy](#) — configures a DSCP color policy

qos dscp-color-map

Configure the DSCP color map.

Syntax

`qos dscp-color-map map-name`

To remove a color map, use the `no qos dscp-color-map map-name` command.

Parameters

map-name

Enter the name of the DSCP color map. The map name can have a maximum of 32 characters.

Defaults

None

Command
Modes

CONFIGURATION

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage
Information

A color map outlines the codepoint mappings to the appropriate color mapping (green, yellow, red) for the traffic. The system uses this information use to handle the traffic on the interface based on the traffic priority and places it into the appropriate shaping queue. You cannot delete a DSCP color map when it is configured on an interface. If you do, all the DSCP values are set to green (low drop precedence). To delete the DSCP color map that is being used by one or more interfaces, remove the DSCP map from each interface.

Example

```
Dell (conf) #qos dscp-color-map mymap
```

Related
Commands

[qos dscp-color-map](#) — associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map

[dscp](#) — sets the number of specific DSCP values for color map profile to yellow or red.

qos dscp-color-policy

Associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map.

Syntax `dscp-color-policy color-map-profile-name`
To remove a color policy map profile, use the `no dscp-color-policy color-map-profile-name` command.

Parameters

<i>color-map-profile-name</i>	Enter the color map profile name. The name can have a maximum of 32 characters.
-------------------------------	---

Defaults **None**

Command Modes CONFIG-INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

Example The following example assigns the color map, **bat-enclave-map**, to interface **te 0/11**.
`Dell(conf)# int te 0/11`
`Dell(conf-if-te-0/11)# qos dscp-color-policy bat-enclave-map`

Related Commands [dscp](#)— sets the number of specific DSCP values for color map profile to yellow or red.
[qos dscp-color-map](#)— configures the DSCP color map.

show qos dscp-color-map

Display the DSCP color map for one or all interfaces.

Syntax `show qos dscp-color-map map-name`

Parameters	<i>map-name</i> Enter the name of the color map.						
Defaults	None						
Command Modes	EXEC						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.5(0.0)</td><td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.						
Example	Display all DSCP color maps. <pre>Dell# show qos dscp-color-map Dscp-color-map mapONE yellow 4,7 red 20,30 Dscp-color-map mapTWO yellow 16,55</pre> Display a specific DSCP color map. <pre>Dell# show qos dscp-color-map mapTWO Dscp-color-map mapTWO yellow 16,55</pre>						
Related Commands	qos dscp-color-map— Configures a DSCP color map.						

Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking operating software supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2).

The implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, refer to the *Dell Networking OS Configuration Guide*.

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

Z9500

Syntax `auto-summary`
To send sub-prefix routing information, use the `no auto-summary` command.

Defaults Enabled.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

clear ip rip

Update all the RIP routes in the system routing table.

Z9500

Syntax	<code>clear ip rip</code>																
Command Modes	EXEC Privilege																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	This command triggers updates of the main RIP routing tables.																

debug ip rip

Examine RIP routing information for troubleshooting.

Z9500

Syntax	<code>debug ip rip [<i>interface</i> database events [<i>interface</i>] trigger]</code> To turn off debugging output, use the <code>no debug ip rip</code> command.				
Parameters	<table><tr><td><i>interface</i></td><td>(OPTIONAL) Enter the interface type and ID as one of the following:</td></tr><tr><td></td><td> - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. </td></tr></table>	<i>interface</i>	(OPTIONAL) Enter the interface type and ID as one of the following:		- For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.
<i>interface</i>	(OPTIONAL) Enter the interface type and ID as one of the following:				
	- For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.				

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

database	(OPTIONAL) Enter the keyword <code>database</code> to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword <code>events</code> to debug only RIP protocol changes.
trigger	(OPTIONAL) Enter the keyword <code>trigger</code> to debug only RIP trigger extensions.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

default-information originate

Generate a default route for the RIP traffic.

Z9500

Syntax

```
default-information originate [always] [metric metric-value]
[route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

Parameters	always	(OPTIONAL) Enter the keyword <code>always</code> to enable the switch software to always advertise the default route.																
	metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 1 to 16. The default is 1 .																
	route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route-map.																
Defaults	Disabled. Metric: 1 .																	
Command Modes	ROUTER RIP																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.6.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced on the E-Series.																	
Usage Information	The default route must be present in the switch routing table for the <code>default-information originate</code> command to take effect.																	

default-metric

Change the default metric for routes. To ensure that all redistributed routes use the same metric value, use this command with the `redistribute` command.

Z9500

Syntax	<code>default-metric <i>number</i></code>	
	To return the default metric to the original values, use the <code>no default-metric</code> command.	
Parameters	<i>number</i>	Specify a number. The range is from 1 to 16. The default is 1 .

Defaults	1																
Command Modes	ROUTER RIP																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	This command ensures that route information being redistributed is converted to the same metric value.																
Related Commands	redistribute — allows you to redistribute routes learned by other methods.																

description

Enter a description of the RIP routing protocol.

Z9500

Syntax	<pre>description {description}</pre> To remove the description, use the <code>no description {description}</code> command.	
Parameters	<i>description</i>	Enter a description to identify the RIP protocol (80 characters maximum).
Defaults	none	
Command Modes	ROUTER RIP	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.7.1.0	Introduced on the E-Series.

Related Commands

[router rip](#) — enters ROUTER mode on the switch.

distance

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights (“administrative distance”) are preferred.

Z9500

Syntax

```
distance weight [ip-address mask [prefix-name]]
```

To return to the default values, use the `no distance weight [ip-address mask]` command.

Parameters

weight	Enter a number from 1 to 255 for the weight (for prioritization). The default is 120 .
ip-address	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.
mask	If you enter an IP address, also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x).
prefix-name	(OPTIONAL) Enter a configured prefix list name.

Defaults

weight = **120**

Command Modes	ROUTER RIP																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Related Commands	default-metric — assigns one distance metric to all routes learned using the <code>redistribute</code> command.																

distribute-list in

Configure a filter for incoming routing updates.

Z9500

Syntax	<pre>distribute-list <i>prefix-list-name</i> in [<i>interface</i>]</pre> To delete the filter, use the <code>no distribute-list <i>prefix-list-name</i> in</code> command.	
Parameters	<i>prefix-list-name</i>	Enter the name of a configured prefix list.
	<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults	Not configured.																		
Command Modes	ROUTER RIP																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.29.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.29.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.29.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																		
8.3.7.0	Introduced on the S4810.																		
7.8.1.0	Introduced on the S-Series.																		
7.6.1.0	Introduced on the C-Series.																		
6.2.1.1	Introduced on the E-Series.																		
Related Commands	ip prefix-list — enters PREFIX-LIST mode and configures a prefix list.																		

distribute-list out

Configure a filter for outgoing routing updates.

Z9500

Syntax	<pre>distribute-list <i>prefix-list-name</i> out [<i>interface</i> bgp connected ospf static]</pre> To delete the filter, use the <code>no distribute-list <i>prefix-list-name</i> out</code> command.	
Parameters	<i>prefix-list-name</i>	Enter the name of a configured prefix list.
	<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

connected	(OPTIONAL) Enter the keyword <code>connected</code> to filter only directly connected routes.
ospf	(OPTIONAL) Enter the keyword <code>ospf</code> to filter all OSPF routes.
static	(OPTIONAL) Enter the keyword <code>static</code> to filter manually configured routes.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands [ip prefix-list](#) — enters PREFIX-LIST mode and configures a prefix list.

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

Z9500

Syntax `ip poison-reverse`
To disable poison reverse, use the `no ip poison-reverse` command.

Defaults	Disabled.																
Command Modes	INTERFACE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Related Commands	ip split-horizon — sets the RIP routing updates to exclude routing prefixes.																

ip rip receive version

To receive specific versions of RIP, set the interface. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.

Z9500

Syntax	<pre>ip rip receive version [1] [2]</pre> To return to the default, use the <code>no ip rip receive version</code> command.				
Parameters	<table> <tr> <td>1</td><td>(OPTIONAL) Enter the number 1 for RIP version 1.</td></tr> <tr> <td>2</td><td>(OPTIONAL) Enter the number 2 for RIP version 2.</td></tr> </table>	1	(OPTIONAL) Enter the number 1 for RIP version 1.	2	(OPTIONAL) Enter the number 2 for RIP version 2.
1	(OPTIONAL) Enter the number 1 for RIP version 1.				
2	(OPTIONAL) Enter the number 2 for RIP version 2.				
Defaults	RIPv1 and RIPv2				
Command Modes	INTERFACE				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.				

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Usage Information	If you want the interface to receive both versions of RIP, use the <code>ip rip receive version 1 2</code> command.	
Related Commands	ip rip send version — sets the RIP version for sending RIP traffic on an interface. version — sets the RIP version the switch software uses.	

ip rip send version

To send a specific version of RIP, set the interface. The version you set on the interface overrides the version command in ROUTER RIP mode.

Z9500

Syntax	<pre>ip rip send version [1] [2]</pre> To return to the default value, use the <code>no ip rip send version</code> command.					
Parameters	1 2	(OPTIONAL) Enter the number 1 for RIP version 1. The default is RIPv1. (OPTIONAL) Enter the number 2 for RIP version 2.				
Defaults	RIPv1					
Command Modes	INTERFACE					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	To enable the interface to send both version of RIP packets, use the <code>ip rip send version 1 2</code> command.
Related Commands	ip rip receive version — sets the RIP version for the interface to receive traffic. version — sets the RIP version for the switch software.

ip split-horizon

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

Z9500

Syntax	<code>ip split-horizon</code> To disable split-horizon, use the <code>no ip split-horizon</code> command.
Defaults	Enabled
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands [ip poison-reverse](#) — sets the prefix for RIP routing updates.

maximum-paths

Set RIP to forward packets over multiple paths.

Z9500

Syntax `maximum-paths number`
To return to the default values, use the `no maximum-paths` commands.

Parameters *number* Enter the number of paths. The range is from 1 to 16. The default is **4** paths.

Defaults **4**

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

Z9500

Syntax

neighbor ip-address

To delete a neighbor setting, use the no neighbor ip-address command.

Parameters

ip-address

Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

To ensure that only specific interfaces are receiving and sending data, use the passive-interface command with the neighbor command.

Related Commands

[passive-interface](#) — sets the interface to only listen to RIP broadcasts.

network

Enable RIP for a specified network. To enable RIP on all networks connected to the switch, use this command.

Z9500

Syntax	<code>network ip-address</code> To disable RIP for a network, use the <code>no network ip-address</code> command.																	
Parameters	<i>ip-address</i>	Specify an IP network address in dotted decimal format. You cannot specify a subnet.																
Defaults	No RIP network is configured.																	
Command Modes	ROUTER RIP																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.6.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced on the E-Series.																	
Usage Information	You can enable an unlimited number of RIP networks. RIP operates over interfaces configured with any address the <code>network</code> command specifies.																	

offset-list

Specify a number to add to the incoming or outgoing route metrics learned using RIP.

Z9500

Syntax `offset-list prefix-list-name {in | out} offset [interface]`
To delete an offset list, use the `no offset-list prefix-list-name {in | out} offset [interface]` command.

Parameters	prefix-list-name	Enter the name of an established Prefix list to determine which incoming routes are modified.
	offset	Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
	interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.

	Version	Description
	6.2.1.1	Introduced on the E-Series.
Usage Information	When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.	
Related Commands	ip prefix-list — enters PREFIX-LIST mode and configure a prefix list.	

output-delay

Set the interpacket delay of successive packets to the same neighbor.

Z9500

Syntax	<code>output-delay delay</code> To return to the switch software defaults for interpacket delay, use the <code>no output-delay</code> command.																	
Parameters	delay	Specify a number of milliseconds as the delay interval. The range is from 8 to 50.																
Defaults	Not configured.																	
Command Modes	ROUTER RIP																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.8.1.0	Introduced on the S-Series.																	
7.6.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced on the E-Series.																	
Usage Information	This command is intended for low-speed interfaces.																	

passive-interface

Suppress routing updates on a specified interface.

Z9500

Syntax	<code>passive-interface interface</code> To delete a passive interface, use the <code>no passive-interface interface</code> command.																			
Parameters	interface	Enter the following information: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.																		
Defaults	Not configured.																			
Command Modes	ROUTER RIP																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																			
8.3.7.0	Introduced on the S4810.																			
7.8.1.0	Introduced on the S-Series.																			
7.6.1.0	Introduced on the C-Series.																			
6.2.1.1	Introduced on the E-Series.																			
Usage Information	Although the passive interface does not send or receive routing updates, the network on that interface still includes in RIP updates sent using other interfaces.																			

Related
Commands

[neighbor](#) — enables RIP for a specified network.

[network](#) — defines a neighbor.

redistribute

Redistribute information from other routing instances.

Z9500

Syntax

```
redistribute {connected | static}
```

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

connected

Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.

static

Enter the keyword `static` to specify that information from static routes is redistributed.

Defaults

Not configured.

Command
Modes

ROUTER RIP

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage
Information

To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

Related
Commands

[default-information originate](#) — generates a default route for RIP traffic.

redistribute isis

Redistribute routing information from an IS-IS instance.

Z9500

Syntax `redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]`

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]` command.

Parameters	tag	(OPTIONAL) Enter the name of the IS-IS routing process.
	level-1	(OPTIONAL) Enter the keywords <code>level-1</code> to redistribute only IS-IS Level-1 routes.
	level-1-2	(OPTIONAL) Enter the keywords <code>level-1-2</code> to redistribute both IS-IS Level-1 and Level-2 routes.
	level-2	(OPTIONAL) Enter the keywords <code>level-2</code> to redistribute only IS-IS Level-2 routes.
	metric metric-value	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 0 to 16.
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced on the E-Series.

redistribute ospf

Redistribute routing information from an OSPF process.

Z9500

Syntax

```
redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]
```

To disable redistribution, use the `no redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]` command.

Parameters	process-id	Enter a number that corresponds to the OSPF process ID to redistribute. The range is from 1 to 65355.
	match external {1 2}	(OPTIONAL) Enter the keywords <code>match external</code> then the numbers 1 or 2 to indicated that external 1 routes or external 2 routes should be redistributed.
	match internal	(OPTIONAL) Enter the keywords <code>match internal</code> to indicate that internal routes should be redistributed.
	metric metric-value	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 0 to 16.
	route-map map-name	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

router rip

To configure and enable RIP, enter ROUTER RIP mode.

Z9500

Syntax	<code>router rip</code> To disable RIP, use the <code>no router rip</code> command.																
Defaults	Disabled.																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.8.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.8.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	To enable RIP, assign a network address using the <code>network</code> command.																
Example	Dell(conf)#<code>router rip</code> Dell(conf-router_rip)#																
Related Commands	network — enables RIP. exit — returns to CONFIGURATION mode.																

show config

Display the changes you made to the RIP configuration. The default values are not shown.

Z9500

Syntax	<code>show config</code>
Command Modes	ROUTER RIP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example	<pre>Dell(conf-router_rip)#show config ! router rip network 172.31.0.0 passive-interface TenGigabitEthernet 0/1 Dell(conf-router_rip)#</pre>
----------------	--

show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

Z9500

Syntax	<code>show ip rip database [<i>ip-address mask</i>]</code>	
Parameters	<i>ip-address</i>	(OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, also enter a mask for that IP address.
	<i>mask</i>	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip rip database` command shown in the following example.

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the routes directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24...	Lists the routes and the sources advertising those routes.

Example

```
Dell#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
    [50/1] via 192.14.1.3, 00:00:12, TenGigabitEthernet 0/15
204.250.54.0/24    auto-summary
203.250.49.0/24
    [50/1] via 192.13.1.3, 00:00:12, TenGigabitEthernet 0/14
203.250.49.0/24    auto-summary
210.250.40.0/24
    [50/2] via 1.1.18.2, 00:00:14, Vlan 18
    [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24    auto-summary
207.250.53.0/24
    [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
    [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
    [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24    auto-summary
208.250.42.0/24
```



```

[50/2] via 1.1.120.2, 00:00:55, Port-channel 20
[50/2] via 1.1.130.2, 00:00:12, Port-channel 30
[50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24      auto-summary

```

show running-config rip

Display the current RIP configuration.

Z9500

Syntax	<code>show running-config rip</code>
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example	<pre> show running-config rip ! router rip distribute-list Test1 in distribute-list Test21 out network 10.0.0.0 passive-interface TenGigabitEthernet 2/0 neighbor 20.20.20.20 redistribute ospf 999 version 2 </pre>
----------------	--

timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times, and flush time.

Z9500

Syntax	<code>timers basic update invalid holddown flush</code> To return to the default settings, use the <code>no timers basic</code> command.							
Parameters	<i>update</i>	Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is from zero (0) to 4294967295. The default is 30 seconds .						
	<i>invalid</i>	Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is 180 seconds .						
	<i>holddown</i>	Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is 180 seconds .						
	<i>flush</i>	Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is from zero (0) to 4294967295. The default is 240 seconds .						
Defaults	• update = 30 seconds • invalid = 180 seconds • holddown = 180 seconds • flush = 240 seconds							
Command Modes	ROUTER RIP							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.8.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Usage Information	If you change the timers on one router, also synchronize the timers on all routers in the RIP domain.	

version

Specify either RIP version 1 or RIP version 2.

Z9500

Syntax	<pre>version {1 2}</pre> To return to the default version setting, use the <code>no version</code> command.	
Parameters	1	Enter the keyword 1 to specify RIP version 1.
	2	Enter the keyword 2 to specify RIP version 2.
Defaults	The system sends RIPv1 and receives RIPv1 and RIPv2.	
Command Modes	ROUTER RIP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

**Related
Commands**

[ip rip receive version](#) — sets the RIP version the interface receives.

[ip rip send version](#) — sets the RIP version the interface sends.

Remote Monitoring (RMON)

Dell Networking operating software remote monitoring (RMON) is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection.

RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, and RFC-3434:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819

RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization



NOTE: Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

rmon alarm

Set an alarm on any MIB object.

Z9500

Syntax

```
rmon alarm number variable interval {delta | absolute} rising-  
threshold value event-number falling-threshold value event-  
number [owner string]
```

To disable the alarm, use the `no rmon alarm number` command.

Parameters

number

Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.

variable

Enter the MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3. The object type must be a 32-bit integer.

<i>interval</i>	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
<i>delta</i>	Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
<i>absolute</i>	Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
<i>rising-threshold value event-number</i>	Enter the keywords <code>rising-threshold</code> then the value (32 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
<i>falling-threshold value event-number</i>	Enter the keywords <code>falling-threshold</code> then the value (32 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
<i>owner string</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults

owner

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

Z9500

Syntax

```
rmon collection history {controlEntry integer} [owner name]
[buckets number] [interval seconds]
```

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry integer}` command.

Parameters

controlEntry <i>integer</i>	Enter the keyword <code>controlEntry</code> to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON history table.
owner <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to record the owner of the RMON group of statistics.
buckets <i>number</i>	(OPTIONAL) Enter the keyword <code>buckets</code> then the number of buckets for the RMON collection history group of statistics. The bucket range is from 1 to 1000. The default is 50 .
interval <i>seconds</i>	(OPTIONAL) Enter the keyword <code>interval</code> then the number of seconds in each polling cycle. The range is from 5 to 3600 seconds. The default is 1800 seconds .

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

Z9500

Syntax `rmon collection statistics {controlEntry integer} [owner name]`
 To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

Parameters

controlEntry <i>integer</i>	Enter the keyword <code>controlEntry</code> to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON statistic table.
owner <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to record the owner of the RMON group of statistics.

Defaults none

Command Modes CONFIGURATION INTERFACE (config-if)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

rmon event

Add an event in the RMON event table.

Z9500

Syntax	<pre>rmon event <i>number</i> [log] [trap <i>community</i>] [description <i>string</i>] [owner <i>name</i>]</pre> To disable RMON on an interface, use the <code>no rmon event <i>number</i> [log] [trap <i>community</i>] [description <i>string</i>]</code> command.											
Parameters	<table><tr><td><i>number</i></td><td>Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.</td></tr><tr><td>log</td><td>(OPTIONAL) Enter the keyword <code>log</code> to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is No log.</td></tr><tr><td>trap <i>community</i></td><td>(OPTIONAL) Enter the keyword <code>trap</code> then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either <code>snmp-trap</code> or <code>log-and-trap</code>. The default is public.</td></tr><tr><td>description <i>string</i></td><td>(OPTIONAL) Enter the keyword <code>description</code> then a string describing the event.</td></tr><tr><td>owner <i>name</i></td><td>(OPTIONAL) Enter the keyword <code>owner</code> then the name of the owner of this event.</td></tr></table>	<i>number</i>	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.	log	(OPTIONAL) Enter the keyword <code>log</code> to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is No log .	trap <i>community</i>	(OPTIONAL) Enter the keyword <code>trap</code> then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either <code>snmp-trap</code> or <code>log-and-trap</code> . The default is public .	description <i>string</i>	(OPTIONAL) Enter the keyword <code>description</code> then a string describing the event.	owner <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the name of the owner of this event.	
<i>number</i>	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.											
log	(OPTIONAL) Enter the keyword <code>log</code> to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is No log .											
trap <i>community</i>	(OPTIONAL) Enter the keyword <code>trap</code> then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either <code>snmp-trap</code> or <code>log-and-trap</code> . The default is public .											
description <i>string</i>	(OPTIONAL) Enter the keyword <code>description</code> then a string describing the event.											
owner <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the name of the owner of this event.											
Defaults	As noted in the <i>Parameters</i> section.											
Command Modes	CONFIGURATION											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.											

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon hc-alarm

Set an alarm on any MIB object.

Z9500

Syntax

```
rmon hc-alarm number variable interval {delta | absolute}
rising-threshold value event-number falling-threshold value
event-number [owner string]
```

To disable the alarm, use the `no rmon hc-alarm number` command.

Parameters

<i>number</i>	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
<i>variable</i>	The MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3 The object type must be a 64-bit integer.
<i>interval</i>	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
<i>delta</i>	Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
<i>absolute</i>	Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
<i>rising-threshold value</i> <i>event-number</i>	Enter the keywords <code>rising-threshold</code> then the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.

	falling-threshold value event-number	Enter the keywords <code>falling-threshold</code> then the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the <code>alarmFallingEventIndex</code> or the <code>alarmTable</code> of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.																
	owner string	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to specify an owner for the alarm. This is the <code>alarmOwner</code> object in the <code>alarmTable</code> of the RMON MIB.																
Defaults	owner																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	

show rmon

Display the RMON running status including the memory usage.

Z9500

Syntax	<code>show rmon</code>
Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell# show rmon
RMON status
  total memory used 218840 bytes.
  ether statistics table: 8 entries, 4608 bytes
  ether history table: 8 entries, 6000 bytes
  alarm table: 390 entries, 102960 bytes
  high-capacity alarm table: 5 entries, 1680 bytes
  event table: 500 entries, 206000 bytes
  log table: 2 entries, 552 bytes
Dell#
```

show rmon alarms

Display the contents of the RMON alarm table.

Z9500

Syntax	<code>show rmon alarms [<i>index</i>] [<i>brief</i>]</code>	
Parameters	<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
	<i>brief</i>	(OPTIONAL) Enter the keyword <code>brief</code> to display the RMON alarm table in an easy-to-read format.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

**Example
(Index)**

```
Dell#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon alarm br
index    SNMP OID
-----
1        1.3.6.1.2.1.1.3
2        1.3.6.1.2.1.1.3
3        1.3.6.1.2.1.1.3
4        1.3.6.1.2.1.1.3
5        1.3.6.1.2.1.1.3
6        1.3.6.1.2.1.1.3
7        1.3.6.1.2.1.1.3
8        1.3.6.1.2.1.1.3
9        1.3.6.1.2.1.1.3
10       1.3.6.1.2.1.1.3
11       1.3.6.1.2.1.1.3
12       1.3.6.1.2.1.1.3
13       1.3.6.1.2.1.1.3
14       1.3.6.1.2.1.1.3
15       1.3.6.1.2.1.1.3
16       1.3.6.1.2.1.1.3
17       1.3.6.1.2.1.1.3
18       1.3.6.1.2.1.1.3
19       1.3.6.1.2.1.1.3
20       1.3.6.1.2.1.1.3
21       1.3.6.1.2.1.1.3
22       1.3.6.1.2.1.1.3
Dell#
```

show rmon events

Display the contents of the RMON event table.

Z9500

Syntax	show rmon events [<i>index</i>] [<i>brief</i>]	
Parameters	<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
	<i>brief</i>	(OPTIONAL) Enter the keyword <i>brief</i> to display the RMON event table in an easy-to-read format.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon event br
index      description
-----
1          1
2          2
3          3
4          4
5          5
```

6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18
19	19
20	20
21	21
22	22

Dell#

show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

Z9500

Syntax	show rmon hc-alarm [<i>index</i>] [<i>brief</i>]	
Parameters	<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
	<i>brief</i>	(OPTIONAL) Enter the keyword <i>brief</i> to display the RMON High-Capacity alarm table in an easy-to-read format.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
  object: 1.3.6.1.2.1.1.3
  sample interval: 5
  sample type: absolute value.
  value: 185638
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 1001, RMON event index: 1
  alarm falling threshold value: positive.
  falling threshold: 999, RMON event index: 6
  alarm sampling failed 0 times.
  alarm owner: 1
  alarm storage type: non-volatile.
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon hc-alarm brief
index      SNMP OID
-----
1          1.3.6.1.2.1.1.3
2          1.3.6.1.2.1.1.3
3          1.3.6.1.2.1.1.3
4          1.3.6.1.2.1.1.3
5          1.3.6.1.2.1.1.3
Dell#
```

show rmon history

Display the contents of the RMON Ethernet history table.

Z9500

Syntax	show rmon history [<i>index</i>] [<i>brief</i>]	
Parameters	<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
	<i>brief</i>	(OPTIONAL) Enter the keyword <i>brief</i> to display the RMON Ethernet history table in an easy-to-read format
Defaults	none	
Command Modes	EXEC	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 TenGigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon history brief
index      ifIndex      interface
-----
6001       100974631    TenGigabitEthernet 1/0
6002       100974631    TenGigabitEthernet 1/0
6003       101236775    TenGigabitEthernet 1/1
6004       101236775    TenGigabitEthernet 1/1
9001       134529054    TenGigabitEthernet 2/0
9002       134529054    TenGigabitEthernet 2/0
9003       134791198    TenGigabitEthernet 2/1
9004       134791198    TenGigabitEthernet 2/1
Dell#
```

show rmon log

Display the contents of the RMON log table.

Z9500

Syntax

```
show rmon log [index] [brief]
```

Parameters

index

(OPTIONAL) Enter the table index number to display just that entry.

	brief	(OPTIONAL) Enter the keyword <code>brief</code> to display the RMON log table in an easy-to-read format.																
Defaults	none																	
Command Modes	EXEC																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.																	
Example (Index)	<pre>Dell#show rmon log 2 RMON log entry, alarm table index 2, log index 1 log time: 14638 (THU AUG 12 22:10:40 2004) description: 2 Dell#</pre>																	
Example (Brief)	<pre>Dell#show rmon log br eventIndex description ----- 2 2 4 4 Dell#</pre>																	

show rmon statistics

Display the contents of RMON Ethernet statistics table.

Z9500

Syntax `show rmon statistics [index] [brief]`

Parameters	<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
	<i>brief</i>	(OPTIONAL) Enter the keyword <i>brief</i> to display the RMON Ethernet statistics table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 TengigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
  1024-1518 bytes packets: 0
  owner: 1
  status: OK
  <high-capacity data>
  HC packets received overflow: 0
  HC packets received: 0
  HC bytes received overflow: 0
  HC bytes received: 0
  HC 64bytes packets overflow: 0
```

```

HC 64bytes packets: 0
HC 65-127 bytes packets overflow: 0
HC 65-127 bytes packets: 0
HC 128-255 bytes packets overflow: 0
HC 128-255 bytes packets: 0
HC 256-511 bytes packets overflow: 0
HC 256-511 bytes packets: 0
HC 512-1023 bytes packets overflow: 0
HC 512-1023 bytes packets: 0
HC 1024-1518 bytes packets overflow: 0
HC 1024-1518 bytes packets: 0
Dell#

```

Example (Brief)

```

Dell#show rmon statistics br
index      ifIndex      interface
-----
6001      100974631     TengigabitEthernet 2/0
6002      100974631     TengigabitEthernet 2/0
6003      101236775     TengigabitEthernet 2/1
6004      101236775     TengigabitEthernet 2/1
9001      134529054     TengigabitEthernet 3/0
9002      134529054     TengigabitEthernet 3/0
9003      134791198     TengigabitEthernet 3/1
9004      134791198     TengigabitEthernet 3/1
Dell#

```

Rapid Spanning Tree Protocol (RSTP)

The Dell Networking operating software implementation of rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

bridge-priority

Set the bridge priority for RSTP.

Z9500

Syntax	<code>bridge-priority priority-value</code> To return to the default value, use the <code>no bridge-priority</code> command.	
Parameters	<i>priority-value</i>	Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is 32768 .
Defaults	32768	
Command Modes	CONFIGURATION RSTP (conf-rstp)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

Z9500

Syntax

```
debug spanning-tree rstp [all | bpdu interface {in | out} |
events]
```

To disable debugging, use the `no debug spanning-tree rstp` command.

Parameters

all

(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.

bpdu interface {in | out}

(OPTIONAL) Enter the keyword `bpdu` to debug the bridge protocol data units.

(OPTIONAL) Enter the keyword `interface` along with the type slot/port of the interface you want displayed. Type slot/port options are the following:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Optionally, enter an `in` or `out` parameter with the optional interface:

- For Receive, enter `in`.
- For Transmit, enter `out`.

events

(OPTIONAL) Enter the keyword `events` to debug RSTP events.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#debug spanning-tree rstp bpdu tengigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

Enter a description of the rapid spanning tree.

Z9500

Syntax

```
description {description}
```

To remove the description, use the `no description {description}` command.

Parameters

description

Enter a description to identify the rapid spanning tree (80 characters maximum).

Defaults

none

Command Modes

SPANNING TREE (The prompt is "config-rstp".)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced.

Related Commands [protocol spanning-tree rstp](#) — enters SPANNING TREE mode on the switch.

disable

Disable RSTP globally on the system.

Z9500

Syntax `disable`
To enable Rapid Spanning Tree Protocol, use the `no disable` command.

Defaults RSTP is disabled.

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands [protocol spanning-tree rstp](#) — enters SPANNING TREE mode on the switch.

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Z9500

Syntax	<code>forward-delay seconds</code> To return to the default setting, use the <code>no forward-delay</code> command.																	
Parameters	seconds	Enter the number of seconds that the system waits before transitioning RSTP to the forwarding state. The range is from 4 to 30. The default is 15 seconds .																
Defaults	15 seconds																	
Command Modes	CONFIGURATION RSTP (conf-rstp)																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.2.1.1	Introduced on the E-Series.																	
Related Commands	hello-time — changes the time interval between BPDUs. max-age — changes the wait time before RSTP refreshes the protocol configuration information.																	

hello-time

Set the time interval between the generation of the RSTP bridge protocol data units (BPDUs).

Z9500

Syntax	<code>hello-time [milli-second] seconds</code> To return to the default value, use the <code>no hello-time</code> command.	
Parameters	seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10 seconds. The default is 2 seconds .
	milli-second	Enter the keywords <code>milli-second</code> to configure a hello time on the order of milliseconds. The range is from 50 to 950 milliseconds
Defaults	2 seconds	
Command Modes	CONFIGURATION RSTP (conf-rstp)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>milli-second</code> option to the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals (x/1000)*256. When you configure millisecond hellos, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.
-------------------	---

Related
Commands

[forward-delay](#) — changes the wait time before RSTP transitions to the Forwarding state.

[max-age](#) — changes the wait time before RSTP refreshes the protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the RSTP bridge.

Z9500

Syntax

`max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

max-age

Enter a number of seconds that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command
Modes

CONFIGURATION RSTP (conf-rstp)

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related
Commands

[forward-delay](#) — changes the wait time before RSTP transitions to the Forwarding state.

[hello-time](#) — changes the time interval between BPDUs.

protocol spanning-tree rstp

To configure RSTP, enter RSTP mode.

Z9500

Syntax	<code>protocol spanning-tree rstp</code> To exit RSTP mode, use the <code>exit</code> command.																
Defaults	Not configured																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Usage Information	RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the <code>no disable</code> command from RSTP mode.																
Example	<pre>Dell(conf)#protocol spanning-tree rstp Dell(config-rstp)##no disable</pre>																
Related Commands	disable — disables RSTP globally on the system.																

show config

View the current configuration for the mode. Only non-default values are displayed.

Z9500

Syntax	show config
Command Modes	CONFIGURATION RSTP (conf-rstp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example	Dell(conf-rstp)#show config ! protocol spanning-tree rstp no disable bridge-priority 16384
---------	--

show spanning-tree rstp

Display the RSTP configuration.

Z9500

Syntax	show spanning-tree rstp [brief] [guard]	
Parameters	brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the RSTP configuration information.
	guard	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added support for the optional <code>guard</code> keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display the port error disable state (EDS) caused by loopback BPDU inconsistency.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show spanning-tree rstp guard` command shown in the following example.

Field	Description
Interface Name	RSTP interface.
Instance	RSTP instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), disabled (DIS), or shut down (EDS Shut).
Guard Type	Types of STP guard configured (Root, Loop, or BPDU guard)

Example (Brief)

```
Dell#show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15
Interface
Name      PortID Prio Cost Sts Cost      Designated
          Bridge ID      PortID
-----
Te 2/0 128.418 128 20000 FWD 20000 16384 0001.e801.6aa8 128.418
Te 2/1 128.419 128 20000 FWD 20000 16384 0001.e801.6aa8 128.419
Te 2/8 128.426 128 20000 FWD 20000 8192 0001.e805.e306 128.130
Te 2/9 128.427 128 20000 BLK 20000 8192 0001.e805.e306 128.131
```

Interface	Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
Te 2/0	Desg	128.418	128	20000	FWD	20000	P2P	Yes	
Te 2/1	Desg	128.419	128	20000	FWD	20000	P2P	Yes	
Te 2/8	Root	128.426	128	20000	FWD	20000	P2P	No	
Te 2/9	Altr	128.427	128	20000	BLK	20000	P2P	No	

Dell#

Example (EDS, LBK)



NOTE: "LBK_INC" (bold) means Loopback BPDU Inconsistency.

```
Dell#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Interface
Name      PortID Prio Cost Sts Cost      Designated
-----
Te 0/0 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257
Interface
Name      Role PortID      Prio Cost Sts Cost Link-type Edge
-----
Te 0/0 ErrDis 128.257 128 20000 EDS 0 P2P No

Dell#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max
hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max
hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occurred 00:00:31
ago on Te 0/0
Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier
128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode
```

Example (Guard)

```
Dell#show spanning-tree rstp guard
Interface
Name      Instance Sts      Guard type
-----
Te 0/1 0      INCON(Root) Rootguard
Te 0/2 0      FWD      Loopguard
Te 0/3 0      BLK      Bpduguard
```

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

Z9500

Syntax	<pre>spanning-tree rstp {cost <i>port-cost</i> edge-port [bpduguard [shutdown-on-violation]] priority <i>priority</i> {loopguard rootguard}}</pre>	
Parameters	cost <i>port-cost</i>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: 10-Gigabit Ethernet interface = 2000 - Port Channel interface with one 10-Gigabit Ethernet = 2000 - Port Channel with two 10 Gigabit Ethernet = 1800
	edge-port	Enter the keywords <code>edge-port</code> to configure the interface as a rapid spanning tree edge port.
	bpduguard	(OPTIONAL) Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.
	shutdown-on-violation	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
	priority <i>priority</i>	Enter keyword <code>priority</code> then a value in increments of 16 as the priority. The range is from 0 to 240. The default is 128 .
	loopguard	Enter the keyword <code>loopguard</code> to enable loop guard on an RSTP port or port-channel interface.
	rootguard	Enter the keyword <code>rootguard</code> to enable root guard on an RSTP port or port-channel interface.
	Defaults	Not configured.
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added support for the optional <code>guard</code> keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the <code>hardware shutdown-on-violation</code> options.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the optional bridge port data unit (BPDU) guard.
6.2.1.1	Introduced on the E-Series.

Usage Information

The `BPDU guard` option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an Error Disable state if a BPDU appears and a message is logged so that the administrator can take corrective action.



NOTE: A port configured as an edge port, on an RSTP switch, immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with a `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message displays: `% Error: RootGuard is configured. Cannot configure LoopGuard.`

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

```
Dell(conf)#interface tengigabitethernet 2/0
Dell(conf-if-te-2/0)#spanning-tree rstp edge-port
Dell(conf-if-te-2/0)#show config
!
interface TenGigabitEthernet 2/0
no ip address
```

```

switchport
spanning-tree rstp edge-port
no shutdown
Dell#

```

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

Z9500

Syntax	tc-flush-standard To disable, use the no tc-flush-standard command.																
Defaults	Disabled																
Command Modes	CONFIGURATION (conf-rstp)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.5.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.5.1.0	Introduced on the E-Series.																
Usage Information	By default, the system implements an optimized flush mechanism for RSTP. This implementation helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this <i>knob</i> command to enable flushing MAC addresses after receiving every topology change notification.																

Security

The commands in this chapter are available on the S5000 switch.

This chapter contains various types of security commands offered in the Dell Networking OS. The commands are listed in the following sections:

- [Role-Based Access Control](#)
- [AAA Accounting Commands](#)
- [Authorization and Privilege Commands](#)
- [Authentication and Password Commands](#)
- [RADIUS Commands](#)
- [TACACS+ Commands](#)
- [SSH Server and SCP Commands](#)
- [Secure DHCP Commands](#)

For configuration details, refer to the Security chapter in the *Dell Networking OS Configuration Guide*.

Role-Based Access Control Commands

With Role-Based Access Control (RBAC), access and authorization is controlled based on a user's role. Users are granted permissions based on their user roles, not on their individual user ID. User roles are created for job functions and through those roles they acquire the permissions to perform their associated job function.

This section describes the syntax and usage of RBAC-specific commands. You can find information on other related security commands in this chapter:

- [aaa accounting](#)
- [aaa authentication login](#)
- [aaa authorization commands](#)
- [authorization](#)
- [show accounting](#)
- [show users](#)
- [username](#)

aaa authorization role-only

Configure authentication to use the user’s role only when determining if access to commands is permitted.

Syntax	aaa authorization role-only To return to the default setting, use the no aaa authentication role-only command.	
Parameters	name inherit existing-role-name	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator). Enter the inherit keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).
Defaults	none	
Command Modes	CONFIGURATION	
Command History	Version 9.5(0.0)	Description Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	By default, access to commands are determined by the user’s role (if defined) or by the user’s privilege level. If the aaa authorization role-only command is enabled, then only the user’s role is used. Before you enable role-based only AAA authorization: 1. Locally define a system administrator user role.This will give you access to login with full permissions even if network connectivity to remote authentication servers is not available. 2. Configure login authentication on the console. This ensures that all users are properly identified through authentication no matter the access point 3. Specify an authentication method (RADIUS, TACACS+, or Local). 4. Specify authorization method (RADIUS, TACACS+ or Local). 5. Verify the configuration has been applied to the console or VTY line.	
Related Commands	login authentication, password, radius-server host, tacacs-server host	

role

Changes command permissions for roles.

Syntax `role mode {{{ addrole | deleterole } role-name } | reset } command`
To delete access to a command, use the `no role mode role-name`

Parameters	mode	Enter one of the following keywords as the mode for which you are controlling access: configure for CONFIGURATION mode exec for EXEC mode interface for INTERFACE modes line for LINE mode route-map for Route-map mode router for Router mode
	addrole	Enter the keyword <code>addrole</code> to add permission to the command. You cannot add or delete rights for the <code>sysadmin</code> role.
	deleterole	Enter the keyword <code>deleterole</code> to remove access to the command. You cannot add or delete rights for the <code>sysadmin</code> role.
	role-name	Enter a text string for the name of the user role up to 63 characters. These are 3 system defined roles you can modify: <code>secadmin</code> , <code>netadmin</code> , and <code>netoperator</code> .
	reset	Enter the keyword <code>reset</code> to reset all roles back to default for that command.
	command	Enter the command's keywords to assign the command to a certain access level. You can enter one or more keywords.

Defaults `none`
Command Modes `CONFIGURATION`

Command History	Version	Description
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Related Commands **userrole**

show role

Display information on permissions assigned to a command, including user role and/or permission level.

Syntax	show role mode {mode} {command}	
Parameters	command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.
	mode mode	Enter keyword then one of the following modes. • configure • exec • interface • line • route-map • router
Defaults	none	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL
Examples	Dell#show role mode configure username Role access: sysadmin	
	Dell#show role mode configure management route Role access: netadmin, sysadmin	
	Dell#show role mode configure management crypto-policy Role access: secadmin, sysadmin	
Related Commands	userrole , username, privilege	

show userroles

Display information on all defined user roles.

Syntax	show userroles	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.
Example	<pre>Dell#show userroles Role Inheritance Modes netoperator netadmin Exec Config Interface Line Router IP Route-map Protocol MAC secadmin Exec Config sysadmin Exec Config Interface Line Router IP Route-map Protocol MAC netoperator testadmin netadmin Exec Config Interface Line Router IP Route-map Protocol MAC</pre>	
Related Commands	userrole , username	

userrole

Create user roles for the role-based security model.

Syntax	userrole <i>name</i> inherit <i>existing-role-name</i>	
	To delete a role name, use the no userrole <i>name</i> command. Note that the reserved role names may not be deleted.	
Parameters	<i>name</i>	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).
	<i>inherit existing-role-name</i>	Enter the <i>inherit</i> keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).
Defaults	none	

Command Modes CONFIGURATION

Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Usage Information Instead of using the system defined user roles, you can create a new user role that best matches your organization. When you create a new user role, you first inherit permissions from one of the system defined roles. Otherwise you would have to create a user role from scratch. You then restrict commands or add commands to that role. For information about this topic, See *Modifying Command Permissions for Roles*.



NOTE: You can change user role permissions on system pre-defined user roles or user-defined user roles.

Important Points to Remember

Consider the following when creating a user role:

- Only the system administrator and user-defined roles inherited from the system administrator can create roles and usernames. Only the system administrator, security administrator, and roles inherited from these can use the `role` command to modify command permissions. The security administrator and roles inherited by security administrator can only modify permissions for commands they already have access to.
- Make sure you select the correct role you want to inherit.



NOTE: If you inherit a user role, you cannot modify or delete the inheritance. If you want to change or remove the inheritance, delete the user role and create it again. If the user role is in use, you cannot delete the user role.

role mode { { { **addrole** | **deleterole** } *role-name* } | **reset** } *command* – Modifies (adds or deletes) command permissions for newly created user roles and system defined roles.

AAA Accounting Commands

AAA Accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services. When you enable AAA Accounting, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA Accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

aaa accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

Z9500

Syntax

```
aaa accounting {system | exec | commands level | role role-name} {name | default}{start-stop | wait-start | stop-only} {tacacs+}
```

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default}{start-stop | wait-start | stop-only} {tacacs+} command`.

Parameters

system	Enter the keyword <code>system</code> to send accounting information of any other AAA configuration.
exec	Enter the keyword <code>exec</code> to send accounting information when a user has logged in to EXEC mode.
commands {level role role-name}	Enter the keyword <code>command</code> then a privilege level for accounting of commands executed at that privilege level or enter the keyword <code>role</code> then the role name for accounting of commands executed by a user with that user role.
name default	Enter one of the following: - For <code>name</code>, enter a user-defined name of a list of accounting methods. - For <code>default</code>, the default accounting methods used.
start-stop	Enter the keywords <code>start-stop</code> to send a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
wait-start	Enter the keywords <code>wait-start</code> to ensure that the TACACS + security server acknowledges the start notice before granting the user's process request.
stop-only	Enter the keywords <code>stop-only</code> to instruct the TACACS+ security server to send a "stop record accounting" notice at the end of the requested user process.
tacacs+	Enter the keyword <code>tacacs+</code> to use TACACS+ data for accounting. The Dell Networking OS currently only supports TACACS+ accounting.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information

In the example below, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1 for example, use the `aaa accounting command 1` command. If you want to track usage by role name for the `secaadmin`, for example, use `aaa accounting command role secaadmin`.

Example

```
Dell(conf)# aaa accounting exec default start-stop tacacs+
Dell(conf)# aaa accounting command 15 default start-stop tacacs+
Dell(conf)# aaa accounting command role secaadmin default start-stop tacacs+
```

Related Commands

[enable password](#) — changes the password for the `enable` command.

[login authentication](#) — enables AAA login authentication on the terminal lines.

[password](#) — creates a password.

[tacacs-server host](#) — specifies a TACACS+ server host.

aaa accounting suppress

Prevent the generation of accounting records of users with the user name value of NULL.

Z9500

Syntax	<pre>aaa accounting suppress null-username</pre> To permit accounting records to users with user name value of NULL, use the <code>no aaa accounting suppress null-username</code> command.
Defaults	Accounting records are recorded for all users.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4280T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information	The system issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the <code>aaa authentication login method-list none</code> command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the <code>aaa accounting suppress</code> command.
--------------------------	--

accounting

Apply an accounting method list to terminal lines.

Z9500

Syntax	<pre>accounting {exec commands {level role role-name} method-list</pre>
---------------	---

Parameters	exec	Enter the keyword <code>exec</code> to apply an EXEC level accounting method list.																				
	commands {<i>level</i> <i>role</i> <i>role-name</i>}	Enter the keywords <code>commands level</code> to apply an EXEC and CONFIGURATION level accounting method list by enter the keyword <code>role</code> and then the role name for accounting of commands executed by a user with that user role.																				
	<i>method-list</i>	Enter a method list that you defined using the <code>aaa accounting exec</code> or <code>aaa accounting commands</code> .																				
Defaults	none																					
Command Modes	LINE																					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Added support for roles on the Z9500.</td></tr><tr><td>9.5(0.0)</td><td>Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.</td></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.3.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.5(0.1)	Added support for roles on the Z9500.	9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.3.1.0	Introduced on the E-Series.
Version	Description																					
9.5(0.1)	Added support for roles on the Z9500.																					
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.																					
9.2(1.0)	Introduced on the Z9500.																					
8.3.11.1	Introduced on the Z9000.																					
8.3.19.0	Introduced on the S4820T.																					
8.3.7.0	Introduced on the S4810.																					
7.6.1.0	Introduced on the S-Series.																					
7.5.1.0	Introduced on the C-Series.																					
6.3.1.0	Introduced on the E-Series.																					
Example	The following example configures accounting for the role <code>secadmin</code> using default <pre>Dell(conf-vty-0)# accounting commands role secadmin default</pre>																					
Related Commands	aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.																					

show accounting

Display the active accounting sessions for each online user.

Z9500

Syntax `show accounting`

Defaults `none`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information This command steps through all active sessions and then displays the accounting records for the active account functions.

Example

```
Dell#show accounting
Active accounted actions on tty2, User guest Priv 1 Role
netoperator
  Task ID 1, EXEC Accounting record, 00:00:30 Elapsed,
service=shell
Active accounted actions on tty3, User admin Priv 15 Role
sysadmin
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed,
service=shell
```

Related Commands [aaa accounting](#) — enables AAA Accounting and creates a record for monitoring the accounting function.

Authorization and Privilege Commands

To set command line authorization and privilege levels, use the following commands.

authorization

Apply an authorization method list to terminal lines.

Z9500

Syntax	<code>authorization {exec commands {level role role-name}} method-list</code>	
Parameters	exec	Enter the keyword <code>exec</code> to apply an EXEC level authorization method list.
	commands {level role role-name}	Enter the keyword <code>commands</code> followed by either a privilege level for accounting of commands executed at that privilege level, or enter the keyword <code>role</code> then the role name for authorization of commands executed by a user with that user role.
	method-list	Enter a method list that you defined using the <code>aaa accounting exec</code> or <code>aaa accounting commands</code> .
Defaults	none	
Command Modes	LINE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Related
Commands

[aaa authorization commands](#) — sets the parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands

[aaa authorization exec](#) — sets the parameters that restrict (or permit) a user's access to EXEC level commands.

aaa authorization commands

Set parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands.

Z9500

Syntax

```
aaa authorization commands {level | role role-name}{name|
default} {local | tacacs+| none}

Undo a configuration with the no aaa authorization commands {level |
role role-name} {name|default} {local | tacacs+ | none}
command.
```

Parameters

commands	Enter the keyword <code>commands</code> then the command privilege level for command level authorization.
level	
role role-name	Enter the keyword <code>role</code> then the role name.
name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword <code>none</code> to apply no authorization.

Defaults

none

Command
Modes

CONFIGURATION

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Added support for RADIUS.

aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

Z9500

Syntax	<pre>aaa authorization config-commands</pre> Disable authorization checking for CONFIGURATION level commands using the <code>no aaa authorization config-commands</code> command.														
Defaults	Enabled when you configure <code>aaa authorization commands</code> command.														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the E-Series.														
Usage Information	By default, the <code>aaa authorization commands</code> command configures the system to check both EXEC level and CONFIGURATION level commands. Use the command <code>no aaa authorization config-commands</code> to enable only EXEC-level command checking.														

aaa authorization exec

Set parameters that restrict (or permit) a user’s access to EXEC-level commands.

Z9500

Syntax aaa authorization exec {*name* | default} {local || tacacs+ || if-authenticated || none}

To disable authorization checking for EXEC level commands, use the no aaa authorization exec command.

Parameters	name	Define a name for the list of authorization methods.
	default	Define the default list of authorization methods.
	local	Use the authorization parameters on the system to perform authorization.
	tacacs+	Use the TACACS+ protocol to perform authorization.
	none	Enter the keyword none to apply no authorization.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Added support for RADIUS.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

Z9500

Syntax `privilege mode {level level command | reset command}`
To delete access to a level and command, use the `no privilege mode level level command command`.

Parameters	mode	Enter one of the following keywords as the mode for which you are controlling access: • <code>configure</code> for CONFIGURATION mode • <code>exec</code> for EXEC mode • <code>interface</code> for INTERFACE modes • <code>line</code> for LINE mode • <code>route-map</code> for ROUTE-MAP mode • <code>router</code> for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes
	level level	Enter the keyword <code>level</code> then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.
	reset	Enter the keyword <code>reset</code> to return the security level to the default setting.
	command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information To define a password for the level to which you are assigning privilege or access, use the `enable password` command.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

Z9500

Syntax	<pre>privilege level level</pre> To delete access to a terminal line, use the <code>no privilege level level</code> command.	
Parameters	level level	Enter the keyword <code>level</code> then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes.
Defaults	<i>level</i> = 15	
Command Modes	LINE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking Command Line Reference Guide</i>	

Version	Description
6.1.1.0	Introduced on the E-Series.

Authentication and Password Commands

To manage access to the system, use the following the commands.

aaa authentication enable

Configure AAA Authentication method lists for user access to EXEC privilege mode (the “Enable” access).

Z9500

Syntax	<pre>aaa authentication enable {default <i>method-list-name</i>} <i>method</i> [... <i>method2</i>]</pre> To return to the default setting, use the <code>no aaa authentication enable {default <i>method-list-name</i>} <i>method</i> [... <i>method2</i>]</code> command.									
Parameters	<table><tr><td>default</td><td>Enter the keyword <code>default</code> then the authentication methods to use as the default sequence of methods for the Enable login. The default is <code>default enable</code>.</td></tr><tr><td><i>method-list-name</i></td><td>Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.</td></tr><tr><td><i>method</i></td><td>Enter one of the following methods: <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. <code>line</code>: use the password the <code>password</code> command defines in LINE mode. <code>none</code>: no authentication. <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. <code>tacacs+</code>: use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command. </td></tr><tr><td><i>... method2</i></td><td>(OPTIONAL) In the event of a “no response” from the first method, the system applies the next configured method.</td></tr></table>	default	Enter the keyword <code>default</code> then the authentication methods to use as the default sequence of methods for the Enable login. The default is <code>default enable</code> .	<i>method-list-name</i>	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.	<i>method</i>	Enter one of the following methods: <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. <code>line</code>: use the password the <code>password</code> command defines in LINE mode. <code>none</code>: no authentication. <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. <code>tacacs+</code>: use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.	<i>... method2</i>	(OPTIONAL) In the event of a “no response” from the first method, the system applies the next configured method.	
default	Enter the keyword <code>default</code> then the authentication methods to use as the default sequence of methods for the Enable login. The default is <code>default enable</code> .									
<i>method-list-name</i>	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.									
<i>method</i>	Enter one of the following methods: <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. <code>line</code>: use the password the <code>password</code> command defines in LINE mode. <code>none</code>: no authentication. <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. <code>tacacs+</code>: use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.									
<i>... method2</i>	(OPTIONAL) In the event of a “no response” from the first method, the system applies the next configured method.									
Defaults	Use the <code>enable password</code> .									
Command Modes	CONFIGURATION									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .									

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

By default, the `Enable password` is used. If you configure `aaa authentication enable default`, the system uses the methods defined for `Enable access` instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

Related Commands

[enable password](#) — changes the password for the `enable` command.

[login authentication](#) — enables AAA login authentication on the terminal lines.

[password](#) — creates a password.

[radius-server host](#) — specifies a RADIUS server host.

[tacacs-server host](#) — specifies a TACACS+ server host.

aaa authentication login

Configure AAA Authentication method lists for user access to EXEC mode (`Enable log-in`).

Z9500

Syntax

```
aaa authentication login {method-list-name | default} method  
[... method4]
```

To return to the default setting, use the `no aaa authentication login {method-list-name | default}` command.

Parameters	<i>method-list-name</i>	Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
	default	Enter the keyword <code>default</code> to specify that the method list specified is the default method for all terminal lines.
	<i>method</i>	Enter one of the following methods: • <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. Not available if role-only is in use. • <code>line</code>: use the password the <code>password</code> command defines in LINE mode. Not available if role-only is in use. • <code>local</code>: use the password for the userid contained in the local password database. • <code>none</code>: no authentication. Not available if role-only is in use. • <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. • <code>tacacs+</code>: use the TACACS+ servers configured with the <code>tacacs-server host</code> command.
	<i>... method4</i>	(OPTIONAL) Enter up to four additional methods. In the event of a "no response" from the first method, the system applies the next configured method (up to four configured methods).

Defaults Not configured (that is, no authentication is performed).

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description						
7.5.1.0	Introduced on the C-Series.						
6.2.1.0	Introduced on the E-Series.						
Usage Information	By default, the locally configured username password is used. If you configure <code>aaa authentication login default</code>, the system uses the methods this command defines for login instead. Methods configured with the <code>aaa authentication login</code> command are evaluated in the order they are configured. If users encounter an error with the first method listed, the system applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user's name is not listed in the local database, the next method is applied. If the correct user name/password combination is not entered, the user is not allowed access to the switch.  NOTE: If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method. After configuring the <code>aaa authentication login</code> command, configure the <code>login authentication</code> command to enable the authentication scheme on terminal lines. Connections to the SSH server work with the following login mechanisms: local, radius, and tacacs.						
Related Commands	login authentication — enables AAA login authentication on the terminal lines. password — creates a password. radius-server host — specifies a RADIUS server host. tacacs-server host — specifies a TACACS+ server host.						

access-class

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

Z9500

Syntax	<code>access-class access-list-name</code> To delete a setting, use the <code>no access-class</code> command.	
Parameters	<i>access-list-name</i>	Enter the name of an established IP Standard ACL.

Defaults	Not configured.																
Command Modes	LINE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Related Commands	line — applies an authentication method list to the designated terminal lines. ip access-list standard — names (or selects) a standard access list to filter based on the IP address. ip access-list extended — names (or selects) an extended access list based on the IP addresses or protocols.																

enable password

Change the password for the `enable` command.

Z9500

Syntax	<pre>enable password [level level] [encryption-type] password</pre> To delete a password, use the <code>no enable password [encryption-type] password [level level]</code> command.	
Parameters	level <i>level</i>	(OPTIONAL) Enter the keyword <code>level</code> then a number as the level of access. The range is from 1 to 15.
	<i>encryption-type</i>	(OPTIONAL) Enter the number 7 or 0 as the encryption type. Enter a 7 then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.

Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.

password Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = **15**.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode) command`.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type "abcd CNTL v]e". When the password is created, you do not use the CNTL + v key combination and enter "abcd]e".



NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands [show running-config](#) — views the current configuration.

[privilege level \(CONFIGURATION mode\)](#) — controls access to the command modes within the switch.

enable restricted

Allows Dell Networking technical support to access restricted commands.

Z9500

Syntax	<code>enable restricted [encryption-type] password</code> To disallow access to restricted commands, use the <code>no enable restricted</code> command.																	
Parameters	<i>encryption-type</i>	(OPTIONAL) Enter the number 7 as the encryption type. Enter 7 followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the <code>show running-config</code> file of another Dell Networking router.																
	<i>password</i>	Enter a text string, up to 32 characters long, as the clear text password.																
Defaults	Not configured.																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	Only Dell Networking Technical Support staff use this command.																	

enable secret

Change the password for the enable command.

Z9500

Syntax	<pre>enable secret [level level] [encryption-type] password</pre> To delete a password, use the <code>no enable secret [encryption-type] password [level level]</code> command.	
Parameters	level level	(OPTIONAL) Enter the keyword <code>level</code> then a number as the level of access. The range is from 1 to 15.
	encryption-type	(OPTIONAL) Enter the number 5 or 0 as the encryption type. Enter a 5 then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the <code>show running-config</code> file of another Dell Networking router.
	password	Enter a text string, up to 32 characters long, as the clear text password.
Defaults	No password is configured. <i>level</i> = 15 .	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode) command`.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type "abcd CNTL v]e". When the password is created, you do not use the CNTL + v key combination and enter "abcd]e".



NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

[show running-config](#) — views the current configuration.

[privilege level \(CONFIGURATION mode\)](#) — controls access to the command modes within the switch.

login authentication

To designate the terminal lines, apply an authentication method list.

Z9500

Syntax

```
login authentication {method-list-name | default}
```

To use the local user/password database for login authentication, use the `no login authentication` command.

Parameters

method-list-name

Enter the keywords `method-list-name` to specify that method list, created in the `aaa authentication login` command, to be applied to the designated terminal line.

default

Enter the keyword `default` to specify that the default method list, created in the `aaa authentication login` command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines. Local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.0	Introduced on the E-Series.																
Usage Information	If you configure the <code>aaa authentication login default</code> command, the <code>login authentication default</code> command automatically is applied to all terminal lines.																
Related Commands	aaa authentication login — selects the login authentication methods.																
password Specify a password for users on terminal lines. Z9500																	
Syntax	<pre>password [encryption-type] password</pre> To delete a password, use the <code>no password password</code> command.																
Parameters	<table> <tr> <td><i>encryption-type</i></td><td> (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the password entered. The options are 0 is the default and means the password is not encrypted and stored as clear text. 7 means that the password is encrypted and hidden. </td></tr> <tr> <td><i>password</i></td><td>Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.</td></tr> </table>	<i>encryption-type</i>	(OPTIONAL) Enter either zero (0) or 7 as the encryption type for the password entered. The options are 0 is the default and means the password is not encrypted and stored as clear text. 7 means that the password is encrypted and hidden.	<i>password</i>	Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.												
<i>encryption-type</i>	(OPTIONAL) Enter either zero (0) or 7 as the encryption type for the password entered. The options are 0 is the default and means the password is not encrypted and stored as clear text. 7 means that the password is encrypted and hidden.																
<i>password</i>	Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.																
Defaults	No password is configured.																
Command Modes	LINE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.																

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The software prompts users for these passwords when the method for authentication or authorization used is "line".

Related Commands

[enable password](#) — sets the password for the `enable` command.

[login authentication](#) — configures an authentication method to log in to the switch.

[service password-encryption](#) — encrypts all passwords configured in the system.

[radius-server key](#) — configures a key for all RADIUS communications between the switch and the RADIUS host server.

[tacacs-server key](#) — configures a key for communication between a TACACS+ server and client.

[username](#) — establishes an authentication system based on user names.

password-attributes

Configure the password attributes (strong password).

Z9500

Syntax

```
password-attributes [min-length number] [max-retry number]
[lockout-period minutes] [character-restriction [upper number]
[lower number] [numeric number] [special-char number]]
```

To return to the default, use the `no password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]` command.

Parameters

min-length <i>number</i>	(OPTIONAL) Enter the keywords <code>min-length</code> then the number of characters. The range is from 0 to 32 characters.
max-retry <i>number</i>	(OPTIONAL) Enter the keywords <code>max-retry</code> then the number of maximum password retries. The range is from 0 to 16.

lockout-period minutes	(OPTIONAL) Enter the keyword <code>lockout-period</code> then the number of minutes. The range is from 1 to 1440 minutes. The default is 0 minutes and the lockout-period is not enabled. This parameter enhances the security of the switch by locking out sessions on the Telnet or SSH sessions for which there has been a consecutive failed login attempts. The console is not locked out.
character- restriction	(OPTIONAL) Enter the keywords <code>character-restriction</code> to indicate a character restriction for the password.
upper number	(OPTIONAL) Enter the keyword <code>upper</code> then the upper number. The range is from 0 to 31.
lower number	(OPTIONAL) Enter the keyword <code>lower</code> then the lower number. The range is from 0 to 31.
numeric number	(OPTIONAL) Enter the keyword <code>numeric</code> then the numeric number. The range is from 0 to 31.
special-char number	(OPTIONAL) Enter the keywords <code>special-char</code> then the number of special characters permitted. The range is from 0 to 31.

Defaults

0 minutes for the lock out period. The lockout-period is not enabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced the <code>lockout-period</code> option on the Z9500.
9.5(0.0)	Introduced the <code>lockout-period</code> option on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Example

In the following example, after 5 un-successful login attempts, the session (SSH/TELNET) goes into a locked state for 5 minutes. If all the 10 sessions are locked out with 5 un-successful attempts in each session, no users can login during the lockout-period.

```
Dell(conf)#password-attributes max-retry 5 lockout-period 5
```

Related Commands

[password](#) — specifies a password for users on terminal lines.

service password-encryption

Encrypt all passwords configured in the system.

Z9500

Syntax

```
service password-encryption
```

To store new passwords as clear text, use the `no service password-encryption` command.

Defaults

Enabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information



CAUTION: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the `no password password` command.

To keep unauthorized people from viewing passwords in the switch configuration file, use the `service password-encryption` command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the `show running-config` command.

show privilege

View your access level.

Z9500

Syntax `show privilege`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show privilege
Current privilege level is 15
Dell#
```

Related Commands [privilege level \(CONFIGURATION mode\)](#) — assigns access control to different command modes.

show users

Allows you to view information on all users logged into the switch, including privilege level and or user role.

Z9500

Syntax `show users [all]`

Parameters **all** (OPTIONAL) Enter the keyword `all` to view all terminal lines in the switch.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show users` command shown in the following example.

Field	Description
(untitled)	Indicates with an asterisk (*) which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.

Field	Description
Location	Displays the IP address of the user.

Example

```
Dell#show users
Authorization Mode:  role or privilege

Line          User      Role      Privilege Host(s) Location
0 console 0    admin    sysadmin   15      idle
*3 vty 1     sec1     secadmin  14      idle   172.31.1.4
4 vty 2     m11     netadmin  12      idle   172.31.1.5
```

Related Commands [username](#) — enables a user.

timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

Z9500

Syntax

```
timeout login response seconds
```

To return to the default values, use the `no timeout login response` command.

Parameters

seconds Enter a number of seconds the software waits before logging you out. The range is:

- VTY: the range is from 1 to 30 seconds, the default is **30 seconds**.
- Console: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).
- AUX: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).

Defaults

See the defaults settings shown in *Parameters*.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is "password" you can enter "p" and wait 29 seconds to enter the next letter.

username

Establish an authentication system based on user names.

Z9500

Syntax

```
username name [access-class access-list-name] [nopassword |
{password | secret} [encryption-type] password] [privilege
level] [role role-name]
```

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the `no username name` command.

Parameters

<i>name</i>	Enter a text string for the name of the user up to 63 characters.
<i>access-class</i> <i>access-list-name</i>	Enter the keywords <code>access-class</code> then the name of a configured access control list (either an IP access control list or MAC access control list).
<i>nopassword</i>	Enter the keyword <code>nopassword</code> to specify that the user should not enter a password.
<i>password</i>	Enter the keyword <code>password</code> then the <i>encryption-type</i> or the password.
<i>secret</i>	Enter the keyword <code>secret</code> then the <i>encryption-type</i> or the password.
<i>encryption-type</i>	Enter an encryption type for the <i>password</i> that you enter. 0 directs the system to store the password as clear text. It is the default encryption type when using the <code>password</code> option. 7 to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the <code>password</code> option only. 5 to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is

available with the `secret` option only, and is the default encryption type for this option.

<i>password</i>	Enter a string up to 32 characters long.
<i>privilege level</i>	Enter the keyword <code>privilege</code> then a number from zero (0) to 15.
<i>role role-name</i>	Enter the keyword <code>role</code> followed by the role name to associate with that user ID.
<i>secret</i>	Enter the keyword <code>secret</code> then the encryption type.

Defaults The default encryption type for the `password` option is **0**. The default encryption type for the `secret` option is **0**.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added support for the <code>secret</code> option and the MD5 password encryption. Extended the name from 25 to 63 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information To view the defined user names, use the `show running-config user` command.

Related Commands [password](#) — specifies a password for users on terminal lines.

[show running-config](#) — views the current configuration.

RADIUS Commands

The Dell Networking OS supports the following RADIUS commands.

debug radius

View RADIUS transactions to assist with troubleshooting.

Z9500

Syntax	<code>debug radius</code> To disable debugging of RADIUS, use the <code>no debug radius</code> command.
Defaults	Disabled.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

ip radius source-interface

Specify an interface's IP address as the source IP address for RADIUS connections.

Z9500

Syntax	<code>ip radius source-interface interface</code> To delete a source interface, use the <code>no ip radius source-interface</code> command.
Parameters	<i>interface</i> Enter the following keywords and slot/port or number information: For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16838.

- For the Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

radius-server deadline

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Z9500

Syntax `radius-server deadline seconds`
To disable this function or return to the default value, use the `no radius-server deadline` command.

Parameters `seconds` Enter a number of seconds during which non-responsive RADIUS servers are skipped. The range is from 0 to 2147483647 seconds. The default is **0 seconds**.

Defaults	0 seconds																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.1.1.0	Introduced on the E-Series.																

radius-server host

Configure a RADIUS server host.

Z9500

Syntax

```
radius-server host {hostname | ipv4-address | ipv6-address}  
[auth-port port-number] [retransmit retries] [timeout seconds]  
[key [encryption-type] key]
```

Parameters

hostname	Enter the name of the RADIUS server host.
ipv4-address ipv6-address	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X::X) of the RADIUS server host.
auth-port port-number	(OPTIONAL) Enter the keywords <code>auth-port</code> then a number as the port number. The range is from zero (0) to 65535. The default port-number is 1812 .
retransmit retries	(OPTIONAL) Enter the keyword <code>retransmit</code> then a number as the number of attempts. This parameter overwrites the <code>radius-server retransmit</code> command. The range is from zero (0) to 100. The default is 3 attempts .
timeout seconds	(OPTIONAL) Enter the keyword <code>timeout</code> then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the <code>radius-server timeout</code> command. The range is from 0 to 1000. The default is 5 seconds .

	key [encryption-type] key (OPTIONAL) Enter the keyword <code>key</code> then an optional encryption-type and a string up to 42 characters long as the authentication key. The RADIUS host server uses this authentication key and the RADIUS daemon operating on this switch. For the encryption-type, enter either zero (0) or 7 as the encryption type for the key entered. The options are: 0 is the default and means the password is not encrypted and stored as clear text. 7 means that the password is encrypted and hidden. Configure this parameter last because leading spaces are ignored.																				
Defaults	Not configured.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.4.1.0</td><td>Added support for IPv6.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Authentication key length increased to 42 characters.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.4.1.0	Added support for IPv6.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Authentication key length increased to 42 characters.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.4.1.0	Added support for IPv6.																				
8.3.7.0	Introduced on the S4810.																				
7.7.1.0	Authentication key length increased to 42 characters.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.2.1.0	Introduced on the E-Series.																				
Usage Information	To configure any number of RADIUS server hosts for each server host that is configured, use this command. The system searches for the RADIUS hosts in the order they are configured in the software. The global default values for the <code>timeout</code>, <code>retransmit</code>, and <code>key</code> optional parameters are applied, unless those values are specified in the <code>radius-server host</code> or other commands. To return to the global default values, if you configure the <code>timeout</code>, <code>retransmit</code>, or <code>key</code> values, include those keywords when using the <code>no radius-server host</code> command syntax.																				

Related
Commands

- [login authentication](#) — sets the database to be checked when a user logs in.
- [radius-server key](#) — sets an authentication key for RADIUS communications.
- [radius-server retransmit](#) — sets the number of times the RADIUS server attempts to send information.
- [radius-server timeout](#) — sets the time interval before the RADIUS server times out.

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

Z9500

Syntax

```
radius-server key [encryption-type] key
```

To delete a password, use the `no radius-server key` command.

Parameters

encryption-type

(OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered. The options are:

- 0 is the default and means the key is not encrypted and stored as clear text.
- 7 means that the key is encrypted and hidden.

key

Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults

Not configured.

Command
Modes

CONFIGURATION

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Authentication key length increased to 42 characters.
7.6.1.0	Introduced on the S-Series.

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	7.5.1.0	Introduced on the C-Series.	6.2.1.0	Introduced on the E-Series.
Version	Description						
7.5.1.0	Introduced on the C-Series.						
6.2.1.0	Introduced on the E-Series.						
Usage Information	The key configured on the switch must match the key configured on the RADIUS server daemon. If you configure the <code>key</code> parameter in the <code>radius-server host</code> command, the key configured with the <code>radius-server key</code> command is the default key for all RADIUS communications.						
Related Commands	radius-server host — configures a RADIUS host.						

radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

Z9500

Syntax	<pre>radius-server retransmit <i>retries</i></pre> To configure zero retransmit attempts, use the <code>no radius-server retransmit</code> command. To return to the default setting, use the <code>radius-server retransmit 3</code> command.								
Parameters	<table> <tr> <td><i>retries</i></td><td>Enter a number of attempts that the system tries to locate a RADIUS server. The range is from zero (0) to 100. The default is 3 retries.</td></tr> </table>	<i>retries</i>	Enter a number of attempts that the system tries to locate a RADIUS server. The range is from zero (0) to 100. The default is 3 retries .						
<i>retries</i>	Enter a number of attempts that the system tries to locate a RADIUS server. The range is from zero (0) to 100. The default is 3 retries .								
Defaults	3 retries								
Command Modes	CONFIGURATION								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.
Version	Description								
9.2(1.0)	Introduced on the Z9500.								
8.3.19.0	Introduced on the S4820T.								
8.3.11.1	Introduced on the Z9000.								

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Related Commands [radius-server host](#) — configures a RADIUS host.

radius-server timeout

To reply to a request, configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server .

Z9500

Syntax `radius-server timeout seconds`
 To return to the default value, use the `no radius-server timeout` command.

Parameters **seconds** Enter the number of seconds between an unsuccessful attempt and when the system times out. The range is from zero (0) to 1000 seconds. The default is **5 seconds**.

Defaults **5 seconds**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Related Commands [radius-server host](#) — configures a RADIUS host.

TACACS+ Commands

The Dell Networking OS supports TACACS+ as an alternate method for login authentication.

debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

Z9500

Syntax	<code>debug tacacs+</code> To disable debugging of TACACS+, use the <code>no debug tacacs+</code> command.
Defaults	Disabled.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

ip tacacs source-interface

Specify an interface's IP address as the source IP address for TACACS+ connections.

Z9500

Syntax	<code>ip tacacs source-interface <i>interface</i></code> To delete a source interface, use the <code>no ip tacacs source-interface</code> command.		
Parameters	<table><tr><td><i>interface</i></td><td>Enter the following keywords and slot/port or number information: For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16838. </td></tr></table>	<i>interface</i>	Enter the following keywords and slot/port or number information: For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16838.
<i>interface</i>	Enter the following keywords and slot/port or number information: For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16838.		

- For the Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

tacacs-server host

Specify a TACACS+ host.

Z9500

Syntax `tacacs-server host {hostname | ipv4-address | ipv6-address} [port number] [timeout seconds] [key key]`

Parameters

hostname	Enter the name of the TACACS+ server host.
ipv4-address ipv6-address	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the TACACS+ server host.
port number	(OPTIONAL) Enter the keyword <code>port</code> then a number as the port to be used by the TACACS+ server. The range is from zero (0) to 65535. The default is 49 .

	timeout seconds (OPTIONAL) Enter the keyword <code>timeout</code> then the number of seconds the switch waits for a reply from the TACACS+ server. The range is from 0 to 1000. The default is 10 seconds. key <i>key</i> (OPTIONAL) Enter the keyword <code>key</code> then a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the <code>tacacs-server key</code> for the TACACS+ daemon.																				
Defaults	Not configured.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.4.1.0</td><td>Added support for IPv6.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Authentication key length increased to 42 characters.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.4.1.0	Added support for IPv6.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Authentication key length increased to 42 characters.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.4.1.0	Added support for IPv6.																				
8.3.7.0	Introduced on the S4810.																				
7.7.1.0	Authentication key length increased to 42 characters.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
6.2.1.1	Introduced on the E-Series.																				
Usage Information	To list multiple TACACS+ servers to be used by the <code>aaa authentication login</code> command, configure this command multiple times. If you are not configuring the switch as a TACACS+ server, you do not need to configure the <code>port</code>, <code>timeout</code> and <code>key</code> optional parameters. If you do not configure a key, the key assigned in the <code>tacacs-server key</code> command is used.																				
Related Commands	aaa authentication login — specifies the login authentication method. tacacs-server key — configures a TACACS+ key for the TACACS server.																				

tacacs-server key

Configure a key for communication between a TACACS+ server and a client.

Z9500

Syntax	<code>tacacs-server key [<i>encryption-type</i>] key</code> To delete a key, use the <code>no tacacs-server key key</code> command.																			
Parameters	<i>encryption-type</i>	(OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered. The options are: • 0 is the default and means the key is not encrypted and stored as clear text. • 7 means that the key is encrypted and hidden.																		
	<i>key</i>	Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.																		
Defaults	Not configured.																			
Command Modes	CONFIGURATION																			
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.0</td><td>Authentication key length increased to 42 characters.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Authentication key length increased to 42 characters.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																			
9.2(1.0)	Introduced on the Z9500.																			
8.3.19.0	Introduced on the S4820T.																			
8.3.11.1	Introduced on the Z9000.																			
8.3.7.0	Introduced on the S4810.																			
7.7.1.0	Authentication key length increased to 42 characters.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.2.1.1	Introduced on the E-Series.																			
Usage Information	The key configured with this command must match the key configured on the TACACS+ daemon.																			

Port Authentication (802.1X) Commands

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

Important Points to Remember

The system limits network access for certain users by using VLAN assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

dot1x authentication (Configuration)

Enable dot1x globally; dot1x must be enabled both globally and at the interface level.

Z9500

Syntax	<code>dot1x authentication</code>
	To disable dot1x on globally, use the <code>no dot1x authentication</code> command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands [dot1x authentication \(Interface\)](#) — enables dot1x on an interface.

dot1x authentication (Interface)

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

Z9500

Syntax `dot1x authentication`
To disable dot1x on an interface, use the `no dot1x authentication` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands [dot1x authentication \(Configuration\)](#) — enables dot1x globally.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

Z9500

Syntax

dot1x auth-fail-vlan *vlan-id* [max-attempts *number*]
To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan vlan-id [max-attempts number]` command.

Parameters

vlan-id

Enter the VLAN Identifier. The range is from 1 to 4094.

max-attempts
number

(OPTIONAL) Enter the keywords `max-attempts` then number of attempts desired before authentication fails. The range is from 1 to 5. The default is **3**.

Defaults

3 attempts

Command Modes

CONFIGURATION (conf-if-interface-slot/port)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface is moved to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next re-authentication interval (`dot1x reauthentication`).

Related Commands

[dot1x port-control](#) — enables port-control on an interface.

[dot1x guest-vlan](#) — configures a guest VLAN for non-dot1x devices.

[show dot1x interface](#) — displays the 802.1X information on an interface.

dot1x auth-server

Configure the authentication server to RADIUS.

Z9500

Syntax `dot1x auth-server radius`

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

Z9500

Syntax `dot1x guest-vlan vlan-id`
To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

Parameters ***vlan-id*** Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION (conf-if-interface-slot/port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Usage Information

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication for the device occurs at the next re-authentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).



NOTE: The layer 3 portion of guest VLAN and authentication fail VLANs can be created regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands

[dot1x auth-fail-vlan](#) — configures a VLAN for authentication failures.

[dot1x reauthentication](#) — enables periodic re-authentication.

[show dot1x interface](#) — displays the 802.1X information on an interface.

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

Z9500

Syntax [no] dot1x mac-auth-bypass

Defaults Disabled

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Introduced on the C-Series and S-Series.

Usage Information To disable MAC authentication bypass on a port, enter the `no dot1x mac-auth-bypass` command.

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

Z9500

Syntax `dot1x max-eap-req number`
To return to the default, use the `no dot1x max-eap-req` command.

Parameters *number* Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related [interface range](#) — configures a range of interfaces.
Commands

dot1x port-control

Enable port control on an interface.

Z9500

Syntax	dot1x port-control {force-authorized auto force-unauthorized}															
Parameters	force-authorized	Enter the keywords <code>force-authorized</code> to forcibly authorize a port.														
	auto	Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.														
	force-unauthorized	Enter the keywords <code>force-unauthorized</code> to forcibly de-authorize a port.														
Defaults	none															
Command Modes	INTERFACE															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.6.1.0	Introduced on the C-Series and S-Series.															
7.4.1.0	Introduced on the E-Series.															
Usage Information	The authenticator performs authentication only when <code>port-control</code> is set to <code>auto</code> .															

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

Z9500

Syntax dot1x quiet-period *seconds*

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters	seconds	Enter the number of seconds. The range is from 1 to 65535. The default is 30 .
------------	----------------	---

Defaults	30 seconds
----------	-------------------

Command Modes	INTERFACE
---------------	-----------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauthentication

Enable periodic re-authentication of the client.

Z9500

Syntax	<code>dot1x reauthentication [interval seconds]</code> To disable periodic re-authentication, use the <code>no dot1x reauthentication</code> command.
--------	--

Parameters	interval seconds	(Optional) Enter the keyword <code>interval</code> then the interval time, in seconds, after which re-authentication is initiated. The range is from 1 to 31536000 (1 year). The default is 3600 (1 hour) .
------------	-------------------------	--

Defaults	3600 seconds (1 hour)
----------	------------------------------

Command Modes	INTERFACE
---------------	-----------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
-----------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands [interface range](#) — configures a range of interfaces.

dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

Z9500

Syntax `dot1x reauth-max number`
 To return to the default, use the `no dot1x reauth-max` command.

Parameters *number* Enter the permitted number of re-authentications. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

Z9500

Syntax	<code>dot1x server-timeout seconds</code> To return to the default, use the <code>no dot1x server-timeout</code> command.	
Parameters	seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30 .
Defaults	30 seconds	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

Z9500

Syntax	<code>dot1x supplicant-timeout seconds</code> To return to the default, use the <code>no dot1x supplicant-timeout</code> command.	
Parameters	seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30 .

Defaults	30 seconds														
Command Modes	INTERFACE														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the C-Series and S-Series.	7.4.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the C-Series and S-Series.														
7.4.1.0	Introduced on the E-Series.														

dot1x tx-period

Configure the intervals at which EAPOL PDUs are transmitted by the Authenticator PAE.

Z9500

Syntax	<code>dot1x tx-period <i>seconds</i></code> To return to the default, use the <code>no dot1x tx-period</code> command.									
Parameters	<i>seconds</i>	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 31536000 (1 year). The default is 30 .								
Defaults	30 seconds									
Command Modes	INTERFACE									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.
Version	Description									
9.2(1.0)	Introduced on the Z9500.									
8.3.19.0	Introduced on the S4820T.									
8.3.11.1	Introduced on the Z9000.									

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

show dot1x interface

Display the 802.1X information on an interface.

Z9500

Syntax	<code>show dot1x interface <i>interface</i></code>	
Parameters	<i>interface</i>	Enter one of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	none	
Command Modes	- EXEC - EXEC privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Example	<pre>Dell#show dot1x int Te 2/32 802.1x information on Te 2/32: ----- Dot1x Status: Enable Port Control: AUTO Port Auth Status: UNAUTHORIZED Re-Authentication: Disable</pre>
---------	--

```

Untagged VLAN id:      None
Guest VLAN:           Enable
Guest VLAN id:        10
Auth-Fail VLAN:       Enable
Auth-Fail VLAN id:    11
Auth-Fail Max-Attempts: 3
Tx Period:            30 seconds
Quiet Period:         60 seconds
ReAuth Max:           2
Supplicant Timeout:   30 seconds
Server Timeout:       30 seconds
Re-Auth Interval:     3600 seconds
Max-EAP-Req:          2
Auth Type:            SINGLE_HOST
Auth PAE State:       Initialize
Backend State:        Initialize
Dell#

```

SSH Server and SCP Commands

The Dell Networking OS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

crypto key generate

Generate keys for the SSH server.

Z9500

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
crypto key generate {rsa | rsa1}
```

Parameters

rsa

Enter the keyword `rsa` then the key size to generate a SSHv2 RSA host keys. The range is from 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is **1024**.



NOTE: You must have a license to access the FIPS mode. For more information, contact your Dell Networking representative.

rsa1

Enter the keyword `rsa1` then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048. The default is **1024**.



NOTE: This option is not available in FIPS mode.

Defaults

Key size **1024**; if you enable FIPS mode, the key size is **2048**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Added support for FIPS mode on the S4810.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The host keys are required for key-exchange by the SSH server. If the keys are not found when you enable the server (`ip ssh server enable`), the keys are automatically generated.

This command requires user interaction and generates a prompt prior to overwriting any existing host keys.



NOTE: Only a user with superuser permissions should generate host-keys.

Example

```
Dell#conf
Dell(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024

Host key already exists. Do you want to replace. [y/n] :y
Dell(conf)#
```

Related Commands

[ip ssh server](#) — enables the SSH server.

[show crypto](#) — displays the SSH host public keys.

crypto key zeroize rsa

Removes the generated RSA host keys and zeroize the key storage location.

Syntax

```
crypto key zeroize rsa
```

Defaults

none

Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.5(0.0)</td><td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.						
Related Commands	crypto key generate — Generate keys for SSH server						

debug ip ssh

Enables collecting SSH debug information.

Z9500

Syntax	<pre>debug ip ssh {client server}</pre> To disable debugging, use the <code>no debug ip ssh {client server}</code> command.													
Parameters	<table><tr><td>client</td><td>Enter the keyword <code>client</code> to enable collecting debug information on the client.</td></tr><tr><td>server</td><td>Enter the keyword <code>server</code> to enable collecting debug information on the server.</td></tr></table>	client	Enter the keyword <code>client</code> to enable collecting debug information on the client.	server	Enter the keyword <code>server</code> to enable collecting debug information on the server.									
client	Enter the keyword <code>client</code> to enable collecting debug information on the client.													
server	Enter the keyword <code>server</code> to enable collecting debug information on the server.													
Defaults	Disabled on both client and server.													
Command Modes	EXEC													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.6.1.0	Introduced on the S-Series.													

	Version	Description
	7.5.1.0	Introduced on the C-Series.
	6.1.1.0	Introduced on the E-Series.
Usage Information	Debug information includes details for key-exchange, authentication, and established session for each connection.	

ip scp topdir

Identify a location for files used in secure copy transfer.

Z9500

Syntax	<code>ip scp topdir <i>directory</i></code> To return to the default setting, use the <code>no ip scp topdir</code> command.																	
Parameters	<i>directory</i>	Enter a directory name.																
Defaults	The internal flash (<code>flash:</code>) is the default directory.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	To configure the switch as an SCP server, use the <code>ip ssh server</code> command.																	
Related Commands	ip ssh server — enables the SSH and SCP server on the switch.																	

ip ssh authentication-retries

Configure the maximum number of attempts that should be used to authenticate a user.

Z9500

Syntax	ip ssh authentication-retries 1-10																	
Parameters	1-10	Enter the number of maximum retries to authenticate a user. The range is from 1 to 10. The default is 3 .																
Defaults	3																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	This command specifies the maximum number of attempts to authenticate a user on an SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.																	

ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

Z9500

Syntax	<code>ip ssh connection-rate-limit 1-10</code>	
Parameters	1-10	Enter the number of maximum numbers of incoming SSH connections allowed per minute. The range is from 1 to 10 per minute. The default is 10 per minute .

Defaults	10 per minute																
Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.1.1.0	Introduced on the E-Series.																

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

Z9500

Syntax	<pre>ip ssh hostbased-authentication enable</pre> To disable hostbased-authentication for SSHv2 server, use the <code>no ip ssh hostbased-authentication enable</code> command.							
Parameters	enable	Enter the keyword <code>enable</code> to enable hostbased-authentication for SSHv2 server.						
Defaults	Disabled.							
Command Modes	CONFIGURATION							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.
Version	Description							
9.2(1.0)	Introduced on the Z9500.							
8.3.19.0	Introduced on the S4820T.							

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you enable this command, clients can log in without a password prompt. This command provides two levels of authentication:

- rhost-authentication is done with the file specified in the `ip ssh rhostfile` command.
- checking client host-keys is done with the file specified in the `ip ssh pub-key-file` command.



NOTE: Administrators must specify the two files (`rhosts` and `pub-key-file`) to configure host-based authentication.

Related Commands

[ip ssh pub-key-file](#) — public keys of trusted hosts from a file.

[ip ssh rhostsfile](#) — trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

Z9500

Syntax

```
ip ssh key-size 512-869
```

Parameters

512-869 Enter the key-size number for the server-generated RSA SSHv1 key. The range is from 512 to 869. The default is **768**.

Defaults

Key size **768**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The server-generated key is used for SSHv1 key-exchange.

ip ssh password-authentication

Enable password authentication for the SSH server.

Z9500

Syntax `ip ssh password-authentication enable`
To disable password-authentication, use the `no ip ssh password-authentication enable` command.

Parameters **enable** Enter the keyword `enable` to enable password-authentication for the SSH server.

Defaults Enabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820t.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information	With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.
--------------------------	---

ip ssh pub-key-file

Specify the file used for host-based authentication.

Z9500

Syntax	<code>ip ssh pub-key-file {WORD}</code>
Parameters	WORD Enter the file name for the host-based authentication.
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information	This command specifies the file used for the host-based authentication. The <code>creates/</code> file overwrites the <code>flash://ADMIN_DIR/ssh/knownhosts</code> file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.
--------------------------	---

The file contains the OpenSSH-compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui
+DWEc3cgYAcU5LailMU2ODrzhCwyDNp05tKBU3t
ReGlo8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdhf3Lk4D460HZRhVrxqeNxPDpEn WIMPJi0ds=
ashwani@poclab4
```



NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the chassis.

Example

```
Dell#conf
Dell(conf)# ip ssh pub-key-file flash://knownhosts
Dell(conf)#
```

Related Commands

[show ip ssh client-pub-keys](#) — displays the client-public keys used for the host-based authentication.

ip ssh rekey

Configures the time `rekey-interval` or volume `rekey-limit` threshold at which to re-generate the SSH key during an SSH session.

Syntax

```
ip ssh rekey [time rekey-interval] [volume rekey-limit]
To reset to the default, use no ip ssh rekey [time rekey-interval]
[volume rekey-limit] command.
```

Parameters

time <i>minutes</i>	Enter the keywords time then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is 60 minutes
volume <i>rekey-limit</i>	Enter the keywords volume then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is 1024 megabytes

Defaults

The default time is **60** minutes. The default volume is **1024** megabytes.

Command Modes

CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

ip ssh rhostsfile

Specify the rhost file used for host-based authorization.

Z9500

Syntax	ip ssh rhostsfile {WORD}	
Parameters	WORD	Enter the rhost file name for the host-based authentication.
Defaults	none	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example	Dell#conf Dell(conf)# ip ssh rhostsfile flash://shosts Dell(conf)#
---------	--

Usage Information	This command specifies the rhost file used for host-based authentication. This <code>creates/</code> file overwrites the <code>flash:/ADMIN_DIR/ssh/shosts</code> file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.
-------------------	---

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.



NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the switch.

ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

Z9500

Syntax	<code>ip ssh rsa-authentication enable</code> To disable RSA authentication, use the <code>no ip ssh rsa-authentication enable</code> command.																	
Parameters	enable	Enter the keyword <code>enable</code> to enable RSA authentication for the SSHv2 server.																
Defaults	Disabled.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	Enabling RSA authentication allows the user to log in without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (<code>ip ssh rsa-authentication my-authorized-keys device://filename</code> command).																	
Related Commands	ip ssh rsa-authentication (EXEC) — adds keys for RSA authentication.																	

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

Z9500

Syntax `ip ssh rsa-authentication {my-authorized-keys WORD}`
To delete the authorized keys, use the `no ip ssh rsa-authentication {my-authorized-keys}` command.

Parameters

my-authorized-keys WORD	Enter the keywords <code>my-authorized-keys</code> then the filename of the RSA authorized-keys.
--------------------------------	--

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information If you want to log in without being prompted for a password, log in through RSA authentication. To do that, first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file: `flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).



NOTE: The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/ authorized-keys-username` file.

Related Commands [show ip ssh rsa-authentication](#) — displays the RSA authorized keys.

[ip ssh rsa-authentication \(Config\)](#) — enables RSA authentication.

ip ssh server

Configure an SSH server. The SSH server is enabled by default.

Z9500

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ip ssh server {ciphers cipher-list} {enable | port port-number}  
[kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]
```

To disable SSH server functions, use the `no ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]` command.

Parameters

enable

Enter the key word `enable` to start the SSH server.

ciphers *cipher-list*

Enter the keyword `ciphers` and then a space-delimited list of ciphers that the SSH server supports.

The following ciphers are available.

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

The default cipher list is used.

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

mac *hmac-algorithm*

Enter the keyword `mac` then a space-delimited list of hash message authentication code (HMAC) algorithms supported

by the SSH server for keying hashing for the message authentication.

The following HMAC algorithms are available:

- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-sha2-256`
- `hmac-sha2-256-96`

When FIPS is enabled, the default HMAC algorithm is `hmac-sha1-96`.

When FIPS is not enabled, the default HMAC algorithms are the following:

- `hmac-md5`
- `hmac-md5-96`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-sha2-256`
- `hmac-sha2-256-96`

kex key-exchange-algorithm

Enter the keyword `kex` and then a space-delimited list of key exchange algorithms supported by the SSH server.

The following key exchange algorithms are available:

- `diffie-hellman-group-exchange-sha1`
- `diffie-hellman-group1-sha1`
- `diffie-hellman-group14-sha1`

When FIPS is enabled, the default key-exchange-algorithm is `diffie-hellman-group14-sha1`.

When FIPS is not enabled, the default key-exchange-algorithms are the following:

- `diffie-hellman-group-exchange-sha1`
- `diffie-hellman-group1-sha1,`
- `diffie-hellman-group14-sha1`

port port-number

(OPTIONAL) Enter the keyword `port` then the port number of the listening port of the SSH server. The range is from 1 to 65535. The default is **22**.

[version {1 | 2}]

(OPTIONAL) Enter the keyword `version` then the SSH version 1 or 2 to specify only SSHv1 or SSHv2.



NOTE: If you enable FIPS mode, you can only select version 2.

Defaults

- Default listening port is **22**.
- Default cipher list is 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr.
- When FIPS is enabled, the default is hmac-sha1-96.
- When FIPS is not enabled, the default is hmac-md5,hmac-md5-96,hmac-sha1,hmac-sha1-96,hmac-sha2-256,hmac-sha2-256-96.
- *When FIPS is enabled, the default is diffie-hellman-group14-sha1.*
- When FIPS is not enabled, the default is diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced the <code>cipher</code> , <code>kex</code> and <code>mac</code> options on the Z9500.
9.5(0.0)	Introduced the <code>cipher</code> , <code>kex</code> and <code>mac</code> options on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

Example

```
Dell# conf
Dell(conf)# ip ssh server port 45
Dell(conf)# ip ssh server enable
Dell#
```

Related [show ip ssh](#) — displays the ssh information.
Commands

ip ssh source-interface

Specifies an interface's IP address as the source IP address for an outgoing SSH connections.

Z9500

Syntax `ip ssh source-interface interface`
To delete a source interface, use the `no ip ssh source-interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: - For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> then the slot/port information. - For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16838. - For the Null interface, enter the keywords <code>null 0</code>. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
------------------	--

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S-Series and Z9000.

Usage Information The `source-interface interface` attribute is applicable for both the `SSH client` as well as the `COPY (SCP)` commands. Using these attributes the client session tags an error to the user during run time, in case there is a mismatch between this command and the `ip ssh vrf` command.

Example

```
Dell(config)#ip ssh source-interface tengigabitethernet 0/36
Dell(config)#do ssh 10.10.10.2 -l admin
Dell(config)#no ip ssh source-interface
```

show crypto

Display the public part of the SSH host-keys.

Z9500

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
show crypto key mypubkey {rsa | rsa1}
```

Parameters

Key	Enter the keyword <code>key</code> to display the host public key.
mypubkey	Enter the keyword <code>mypubkey</code> to display the host public key.
rsa	Enter the keyword <code>rsa</code> to display the host SSHv2 RSA public key.
rsa1	Enter the keyword <code>rsa1</code> to display the host SSHv1 RSA public key.



NOTE: If you enable FIPS mode, this parameter is not available.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Example

```
Dell#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtzkZME/
e8V8smnXR22EJGQhCMkEOkuisa+OILVoMYU1ZKGfj0W5BPCSvF/
x5ifqYFFwUzJNOcsJK7vjSsnmMhChF2YSvXlvTJ6h971FJAQlOsgd0ycpocsF
+DNLKfJnx7SAjhakFQMwG
g/g78ZkDT3Ydr8KKjfSI4Bg/WS8B740=

Dell#show crypto key mypubkey rsa1
1024 35
131060015480873398953257515397249657850072206444294963674080935
6830889610203172266
798895675496676526500637962218977992760927852363883922305508181
9166009928132616408
664345774602219229518903992966334579117374224743155375050167692
9660273790601494434
050000015179864425629613385774919236081771341059533760063913083
Dell#
```

Related Commands

[crypto key generate](#) — generates the SSH keys.

show ip ssh

Display information about established SSH sessions.

Z9500

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
show ip ssh
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#sh ip ssh
SSH server           : enabled.
SSH server version   : v1 and v2.
Password Authentication : enabled.
Hostbased Authentication : disabled.
RSA Authentication   : disabled.
Vty Encryption HMAC Remote IP
1 3des-cbc hmac-md5 10.1.20.48
2 3des-cbc hmac-md5 10.1.20.48
```

Related Commands

[ip ssh server](#) — configures an SSH server.

[show ip ssh client-pub-keys](#) — displays the client-public keys.

show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

Z9500

Syntax `show ip ssh client-pub-keys`

Defaults `none`

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

Example

```
Dell#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoiETH09G4sNV+ui
+DWEc3cgYAcU5LailMU2ODrzhCwyDNp05tKBU3tReG1
o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdhf3Lk4D460HZRhhVrxqeNxPDpEnWIMPJi0
```



```
ds= ashwani@poclab4
Dell#
```

Related Commands [ip ssh pub-key-file](#) — configures the filename for the host-based authentication.

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

Z9500

Syntax	<code>show ip ssh rsa-authentication {my-authorized-keys}</code>	
Parameters	my-authorized-keys	Display the RSA authorized keys.
Defaults	none	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command displays the contents of the `flash:/ADMIN_DIR/ssh/authorized-keys.username` file.

Example

```
Dell#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1
X1JOMeO6Nd0WuYzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRcnw/
zCmlnCf0+qVTdl0ofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+U9tMwhS8vy8A
VxdH4x4km3c3t5Jvc=
freedom@poclab4

Dell#
```

ssh

Open an SSH connection specifying the hostname, username, encryption cipher, HMAC algorithm, port number, and version of the SSH client.

Z9500

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ssh[vrf vrf-name] {hostname | ipv4 address | ipv6 address} [-c
encryption cipher | -l username | -m HMAC algorithm | -p port-
number | -v {1 | 2}]
```

Parameters

vrf vrf-name

(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to specify the VRF used with the SSH session.



NOTE: The VRF configured using this command has a higher precedence than the VRF configured using the `ip ssh vrf vrf-name` command. If you do not configure a VRF using this command, then the SSH client uses the configured VRF (if any). If there is a mismatch between VRFs that are configured using the `ip ssh source-interface` command and the `ssh vrf vrf-name` command, then an error is reported.

hostname

(OPTIONAL) Enter the IP address or the host name of the remote device.

vrf instance

(OPTIONAL) E-Series Only: Enter the keyword `vrf` then the VRF Instance name to open an SSH connection to that instance.

ipv4 address

(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.

**ipv6-address
prefix-length**

(OPTIONAL) Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.



NOTE: The `::` notation specifies successive hexadecimal fields of zeros.

**-c encryption
cipher**

Enable the "FIPS mode enable", this mode will support only v2 client.

"no fips mode enable"(disable) will support v1 & v2 client. This comment is applicable for both ciphers & HMAC algorithms:

- 3des-cbc

	• aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr
-l <i>username</i>	(OPTIONAL) Enter the keyword -l then the user name used in this SSH session. The default is the user name of the user associated with the terminal.
-m <i>HMAC algorithm</i>	Enter one of the following HMAC algorithms to use. (For v2 clients only): "no fips mode enable"(disable) will support v1 & v2 client. • hmac-sha1 • hmac-sha1-96 • hmac-md5 • hmac-md5-96 • hmac-sha2-256 • hmac-sha2-256-96
-p <i>port-number</i>	(OPTIONAL) Enter the keyword -p then the port number. The range is from 1 to 65535. The default is 22 .
-v {1 2}	(OPTIONAL) Enter the keyword -v then the SSH version 1 or 2. The default is the version from the protocol negotiation.

Defaults

As shown in the *Parameters* section.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for the following ciphers and HMAC algorithms on the Z9000, S6000, S4820T, S4820T. • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr

	Version	Description • aes256-ctr • hmac-sha2-256 • hmac-sha2-256-96
	9.4(0.0)	Added support for VRF.
	9.2(1.0)	Introduced on the Z9500.
	9.0.2.0	Introduced on the S6000.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.12.0	Added support for the <code>-c</code> and <code>-m</code> parameters on the S4810.
	8.3.7.0	Introduced on the S4810.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Added IPv6 support. Introduced on the C-Series.
	6.1.1.0	Introduced on the E-Series.
Usage Information	Dell Networking OS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.	
Example	<pre> Dell#ssh 10.11.8.12 ? -c Encryption cipher to use (for v2 clients only) -l User name option -m HMAC algorithm to use (for v2 clients only) -p SSH server port option (default 22) -v SSH protocol version <cr> Dell#ssh 10.11.8.12 -c ? 3des-cbc Force ssh to use 3des-cbc encryption cipher Dell#ssh 10.11.8.12 -m ? hmac-sha1 Force ssh to use hmac-sha1 HMAC algorithm hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm hmac-md5 Force ssh to use hmac-md5 HMAC algorithm hmac-md5-96 Force ssh to use hmac-md5-96 HMAC algorithm Dell#ssh vrf vrf1 10.10.10.2 -l admin </pre>	

Secure DHCP Commands

DHCP as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

clear ip dhcp snooping

Clear the DHCP binding table.

Z9500

Syntax `clear ip dhcp snooping binding`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.

ip dhcp relay

Enable Option 82.

Z9500

Syntax `ip dhcp relay information-option [trust-downstream]`

Parameters

trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.
-------------------------	---

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping

Enable DHCP Snooping globally.

Z9500

Syntax	[no] ip dhcp snooping
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information	When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP Snooping, the binding table is deleted and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.
Related Commands	ip dhcp snooping vlan — enables DHCP Snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Z9500

Syntax	<code>[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number</code>	
Parameters	mac address	Enter the keyword <code>mac</code> then the MAC address of the host to which the server is leasing the IP address.
	vlan-id vlan-id	Enter the keywords <code>vlan-id</code> then the VLAN to which the host belongs. The range is from 2 to 4094.
	ip ip-address	Enter the keyword <code>ip</code> then the IP address that the server is leasing.
	interface type	Enter the keyword <code>interface</code> then the type of interface to which the host is connected. - For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
	slot/port	Enter the slot and port number of the interface.
	lease time	Enter the keyword <code>lease</code> then the amount of time the IP address is leased. The range is from 1 to 4294967295.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.
Commands

ip dhcp snooping database

Delay writing the binding table for a specified time.

Z9500

Syntax `ip dhcp snooping database write-delay minutes`

Parameters *minutes* The range is from 5 to 21600.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping database renew

Renew the binding table.

Z9500

Syntax `ip dhcp snooping database renew`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping trust

Configure an interface as trusted.

Z9500

Syntax	[no] ip dhcp snooping trust
Defaults	Untrusted
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp source-address-validation

Enable IP source guard.

Z9500

Syntax	[no] ip dhcp source-address-validation
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

Z9500

Syntax	[no] ip dhcp snooping vlan <i>name</i>	
Parameters	<i>name</i>	Enter the name of a VLAN on which to enable DHCP Snooping.
Defaults	Disabled.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information	When enabled, the system begins creating entries in the binding table for the specified VLANs.
-------------------	--



NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands	ip dhcp snooping trust — configures an interface as trusted.
------------------	--

show ip dhcp snooping

Display the contents of the DHCP binding table.

Z9500

Syntax `show ip dhcp snooping binding`

Defaults none

- Command Modes**
- EXEC
 - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands [clear ip dhcp snooping](#) — clears the contents of the DHCP binding table.

Service Provider Bridging

Service provider bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the *Dell Networking OS Configuration Guide Service Provider Bridging* chapter.

This chapter includes command line information (CLI) for the Dell Networking operating software Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

For more information, refer to [VLAN Stacking](#), [Spanning Tree Protocol \(STP\)](#), and [GARP VLAN Registration \(GVRP\)](#).

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For more information about Stackable VLAN (VLAN-Stacking) commands, refer to [VLAN Stacking](#).
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol [LACP]) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.

debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

Z9500

Syntax

```
debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]
```

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]` command.

Parameters

interface

Enter one of the following interfaces and slot/port information:

	- For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
in out both	Enter the keyword <code>in</code> , <code>out</code> , or <code>both</code> to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
vlan <i>vlan-id</i>	Enter the keyword <code>vlan</code> then the VLAN ID. The range is from 1 to 4094.
count <i>value</i>	Enter the keyword <code>count</code> then the number of debug outputs. The range is from 1 to 100.

Defaults Debug disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series, and E-Series ExaScale.
7.4.1.0	Introduced

protocol-tunnel

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

Z9500

Syntax `protocol-tunnel {rate-limit rate | stp}`
 To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

Parameters	rate-limit <i>rate</i>	Enter the keyword <code>rate-limit</code> followed by a number for the rate-limit for tunneled packets on the VMAN. The range is from 64 to 320.												
	stp	Enter the keyword <code>stp</code> to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.												
Defaults	none													
Command Modes	CONF-IF-VLAN													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.5.1.1</td><td>Added support for 802.1X, E-LMI, GMRP, GVRP, LLDP, LACP, MMRP, MVRP, and OAM 802.3ah protocol traffic to the E-Series ExaScale.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the C-Series, E-Series, and E-Series ExaScale.</td></tr><tr><td>7.4.1.0</td><td>Introduced</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.5.1.1	Added support for 802.1X, E-LMI, GMRP, GVRP, LLDP, LACP, MMRP, MVRP, and OAM 802.3ah protocol traffic to the E-Series ExaScale.	8.2.1.0	Introduced on the C-Series, E-Series, and E-Series ExaScale.	7.4.1.0	Introduced
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.11.1	Introduced on the Z9000.													
8.5.1.1	Added support for 802.1X, E-LMI, GMRP, GVRP, LLDP, LACP, MMRP, MVRP, and OAM 802.3ah protocol traffic to the E-Series ExaScale.													
8.2.1.0	Introduced on the C-Series, E-Series, and E-Series ExaScale.													
7.4.1.0	Introduced													
Example	<pre>Dell#conf Dell(conf)#interface vlan 2 Dell(conf-if-vl-2)#vlan-stack compatible Dell(conf-if-vl-2)#member Te 1/2-3 Dell(conf-if-vl-2)#protocol-tunnel stp Dell(conf-if-vl-2)#protocol-tunnel enable</pre>													
Related Command	show protocol-tunnel — displays tunneling information for all VLANs.													

protocol-tunnel destination-mac

Overwrite the BPDU destination MAC address with a specific value.

Z9500

Syntax	<code>protocol-tunnel destination-mac <i>xstp address</i></code>	
Parameters	stp	Change the default destination MAC address used for L2PT to another value.

Defaults	The default destination MAC is 01:01:e8:00:00:00.														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the C-Series, and S-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the C-Series, and S-Series.	7.4.1.0	Introduced
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.2.1.0	Introduced on the C-Series, and S-Series.														
7.4.1.0	Introduced														
Usage Information	When you enable VLAN-Stacking, no protocol packets are tunneled.														
Related Command	show protocol-tunnel — displays tunneling information for all VLANs.														

protocol-tunnel enable

Enable protocol tunneling globally on the system.

Z9500

Syntax	<pre>protocol-tunnel enable</pre> To disable protocol tunneling, use the <code>no protocol-tunnel enable</code> command.				
Defaults	Disabled.				
Command Modes	CONFIGURATION				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description				
9.2(1.0)	Introduced on the Z9500.				

	Version	Description
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.4.1.0	Introduced
Usage Information	The system must have the default CAM profile with the default microcode before you enable L2PT.	

protocol-tunnel rate-limit

Enable traffic rate limiting per box.

Z9500

Syntax	<pre>protocol-tunnel rate-limit rate</pre> To reset the rate limit to the default, use the <code>no protocol-tunnel rate-limit rate</code> command.	
Parameters	rate	Enter the rate in frames per second. The range is from 75 to 3000. The default is 75 .
Defaults	75 frames per second.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series TeraScale, and E-Series ExaScale. Maximum rate limit on E-Series reduced from 4000 to 3000.
7.4.1.0	Introduced

Example	<pre> Dell# Dell#conf Dell(conf)#protocol-tunnel rate-limit 1000 Dell(conf)# </pre>
Related Commands	show protocol-tunnel — displays tunneling information for all VLANs. show running-config — displays the current configuration.

show protocol-tunnel

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

Z9500

Syntax	<code>show protocol-tunnel [vlan <i>vlan-id</i>]</code>
Parameters	vlan <i>vlan-id</i> (OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.
Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series and E-Series ExaScale.
7.4.1.0	Introduced

Example	<pre> Dell#show protocol-tunnel System Rate-Limit: 75 frames/second VLAN Protocols Interface 1000 STP, PVST Te 1/7, Te 1/6 1001 LLDP, GVRP Te 1/7, Te 1/6 1002 MMRP, MVRP Te 1/7, Te 1/6 1003 LACP, DOT1X Te 1/7, Te 1/6 </pre>
---------	--

```
1004 OAM, PAUSE Te 1/7, Te 1/6
1005 E-LMI Te 1/7, Te 1/6
```

Example
(Specific VLAN)

```
Dell#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface Vlan Protocol(s)
Tel/2 2 STP, PVST
Dell#
```

Related
Commands

[show running-config](#) — displays the current configuration.

sFlow

sFlow monitoring system includes an sFlow Agent and an sFlow Collector.

- The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector.
- The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- Dell Networking recommends that the sFlow Collector be connected to the Dell Networking chassis through a line card port rather than the route processor module (RPM) Management Ethernet port.
- The system exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to many exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- The source virtual local area network (VLAN) field in the extended switch element is not packed if there is a routed packet.
- The destination VLAN field in the extended switch element is not packed if there is a multicast packet.
- The maximum number of packets that can be sampled and processed per second is:
 - 7500 packets when no extended information packing is enabled.
 - 7500 packets when only extended-switch information packing is enabled (refer to [sflow extended-switch enable](#)).

sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

Z9500

Syntax

```
sflow collector {ip-address | ipv6-address} agent-addr {ip-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number]
```

To delete a configured collector, use the `no sflow collector {ip-address | ipv6-address} agent-addr {ipv4-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number]` command.

Parameters	sflow collector ip-address ipv6-address	Enter the IP address of the collector in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	agent-addr ip-address ipv6-address	Enter the keyword <code>agent-addr</code> followed by the sFlow agent IP address in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
	number	(OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is from 0 to 65535. The default is 6343.
	max-datagram-size number	(OPTIONAL) Enter the keyword <code>max-datagram-size</code> then the size number in bytes. The range is from 400 to 1500. The default is 1400 .

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.4.2.3	Added support for IPv6 sFlow collectors and agents on the E-series TeraScale, C-Series, and S-Series.
8.4.1.1	Added support for IPv6 sFlow collectors and agents on the E-series ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.5.1.0	Expanded the <code>no</code> form of the command to mirror the syntax used to configure.
6.2.1.1	Introduced on the E-Series.

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.

In sFlow, the agent address is a single invariant IPv4 or IPv6 address used to identify the agent to the collector. It is usually assigned the address of a loopback interface on the agent, which provides invariance. The agent address is carried as a field in the payload of the sFlow packets.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, the system returns the corresponding configured agent IP in the MIB requests. The system checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, the system generates the following error: `%Error: Different agent-addr attempted for an existing collector.`

sflow enable (Global)

Enable sFlow globally.

Z9500

Syntax

```
sflow enable
```

To disable sFlow, use the `no sflow enable` command.

Defaults	Disabled.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced S-Series Stacking.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced S-Series Stacking.	8.1.1.0	Introduced on the E-Series ExaScale.	7.7.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																				
9.2(1.0)	Introduced on the Z9500.																				
8.3.19.0	Introduced on the S4820T.																				
8.3.11.1	Introduced on the Z9000.																				
8.3.7.0	Introduced on the S4810.																				
8.2.1.0	Introduced S-Series Stacking.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.7.1.0	Introduced on the S-Series.																				
7.6.1.0	Introduced on the C-Series.																				
6.2.1.1	Introduced on the E-Series.																				
Usage Information	sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.																				
Related Commands	sflow enable (Interface) — enables sFlow on interfaces.																				

sflow enable (Interface)

Enable sFlow on interfaces.

Z9500

Syntax	<pre>sflow enable</pre> To disable sFlow, use the <code>no sflow enable</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on S-Series Stacking.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Usage Information	When you enable sFlow on an interface, flow sampling is done on any traffic going out of the interface.	
		NOTE: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.
Related Commands	sflow enable (Global) — turns sFlow on globally.	

sflow extended-switch enable

Enable packing information on a switch only.

Z9500

Syntax	<pre>sflow extended-switch enable</pre> To disable packing information, use the <code>no sflow extended-switch [enable]</code> command.	
Parameters	enable	Enter the keyword <code>enable</code> to enable global extended information.
Defaults	Disabled.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on S-Series Stacking.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	Dell Networking OS version 7.8.1.0 and later enhances the sflow implementation for real time traffic analysis on the E-Series to provide extended gateway information in cases where the destination IP addresses are learned by different routing protocols and for cases where the destination is reachable over ECMP.	
Related Commands	show sflow — displays the sFlow configuration.	

sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

Z9500

Syntax	<code>sflow polling-interval <i>interval value</i></code> To return to the default, use the <code>no sflow polling-interval <i>interval</i></code> command.	
Parameters	<i>interval value</i>	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is 20 seconds .
Defaults	20 seconds	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on S-Series Stacking.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	The polling interval for an interface is the maximum number of seconds between successive samples of counters sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.	
Related Commands	sflow polling-interval (Interface) — sets the polling interval for an interface.	

sflow polling-interval (Interface)

Set the sFlow polling interval at an interface (overrides the global-level setting.)

Z9500

Syntax	<pre>sflow polling-interval <i>interval value</i></pre> To return to the default, use the <code>no sflow polling-interval <i>interval</i></code> command.	
Parameters	<i>interval value</i>	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is the global counter polling interval .
Defaults	The same value as the current global default counter polling interval.	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on S-Series Stacking.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	This command sets the counter polling interval for an interface.	
Related Commands	sflow polling-interval (Global) — globally sets the polling interval.	

sflow sample-rate (Global)

Change the global default sampling rate.

Z9500

Syntax	<code>sflow sample-rate value</code> To return to the default sampling rate, use the <code>no sflow sample-rate</code> command.	
Parameters	value	Enter the sampling rate value. Enter values in powers of 2 only; for example, 4096, 8192, 16384, and so on. The default is 32768 packets .
Defaults	32768 packets	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	Version	Description
	9.2(1.0)	Introduced on the Z9500.
	8.3.19.0	Introduced on the S4820T.
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.2.1.0	Introduced on S-Series Stacking.
	8.1.1.0	Introduced on the E-Series ExaScale.
	7.7.1.0	Introduced on the S-Series.
	7.6.1.0	Introduced on the C-Series.
	7.4.1.0	Introduced on the E-Series.
Usage Information	Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.	
Related Commands	sflow sample-rate (Interface) — changes the interface sampling rate.	

sflow sample-rate (Interface)

Change the interface default sampling rate.

Z9500

Syntax	<pre>sflow sample-rate value</pre> To return to the default sampling rate, use the <code>no sflow sample-rate</code> command.	
Parameters	value	Enter the sampling rate value. For the C-Series and S-Series, the range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, etc. The default is the Global default sampling .
Defaults	The Global default sampling.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

**Usage
Information**

This command changes the sampling rate for an interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.

**Related
Commands**

[sflow sample-rate \(Global\)](#) — changes the sampling rate globally.

show sflow

Display the current sFlow configuration.

Z9500

Syntax

```
show sflow [interface]
```

Parameters

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port-Channel Ethernet interface, enter the keyword `port-channel` then the slot/port information. The range is from 1 to 128.

**Command
Modes**

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example always displays a value of zero.

Example

```
Dell#show sflow
sFlow services are enabled
Global default sampling rate: 32768
Global default counter polling interval: 20
1 collectors configured
Collector IP addr: 133.33.33.53, Agent IP addr: 133.33.33.116,
UDP port: 6343
0 UDP packets exported
0 UDP packets dropped
165 sFlow samples collected
0 sFlow samples dropped due to sub-sampling

Linecard 1 Port set 0 H/W sampling rate 8192
  Te 1/16: configured rate 8192, actual rate 8192, sub-
sampling rate 1
  Te 1/17: configured rate 16384, actual rate 16384, sub-
sampling rate 2
Linecard 3 Port set 1 H/W sampling rate 16384
  Te 2/40: configured rate 16384, actual rate 16384, sub-
sampling rate 1
Dell#
```

show sflow linecard

Display sFlow information for a line card.

Z9500

Syntax `show sflow linecard slot-id`

Parameters

slot number	Enter a slot number to view information on the line-card ports in that slot. The range of Z9500 slot IDs is from 0 to 2.
--------------------	--

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example below always displays a value of zero.

Example

```
Dell# show sflow linecard 0
Linecard 0
  Samples rcvd from h/w           :0
  Total UDP packets exported      :0
  UDP packets exported via RPM    :0
  UDP packets dropped             :0

Dell# show sflow linecard 1
Linecard 1
  Samples rcvd from h/w           :0
  Total UDP packets exported      :0
  UDP packets exported via RPM    :0
  UDP packets dropped             :0

Dell# show sflow linecard 2
Linecard 2
  Samples rcvd from h/w           :0
  Total UDP packets exported      :0
```

```
      UDP packets exported via RPM      :0
      UDP packets dropped                :0
Dell#
```

Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog.

The chapter contains the following sections:

- [SNMP Commands](#)
- [Syslog Commands](#)

SNMP Commands

The following SNMP commands are available in the Dell Networking operating software.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. The system supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. The system sends SNMP traps, which are messages informing an SNMP management system about the network. The system supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
 - SNMP Timeout — greater than 3 seconds.
 - SNMP Retry count — greater than 2 seconds.
- If you want to query an E-Series switch using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on a non-management port on the switch.
- If you want to send SNMP v1/v2/v3 traps from an E-Series using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

show snmp

Display the status of SNMP network elements.

Z9500

Syntax `show snmp`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp
 32685 SNMP packets input
   0 Bad SNMP version errors
   0 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
 96988 Number of requested variables
   0 Number of altered variables
 31681 Get-request PDUs
   968 Get-next PDUs
   0 Set-request PDUs
 61727 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   9 No such name errors
   0 Bad values errors
   0 General errors
 32649 Response PDUs
 29078 Trap PDUs
Dell#
```

Related Commands [snmp-server community](#) — enables the SNMP and set community string.

show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

Z9500

Syntax `show snmp engineID`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID      IP-addr      Port
80001F88043132333435  172.31.1.3   5009
80001F88043938373635  172.31.1.3   5008

Dell#
```

Related Commands [snmp-server engineID](#) — configures local and remote SNMP engines on the router.

show snmp group

Display the group name, security model, status, and storage type of each group.

Z9500

Syntax `show snmp group`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following Example displays a group named *ngroup*. The *ngroup* has a security model of version 3 (v3) with authentication (*auth*), the read and notify name is *nview* with no write view name specified, and finally the row status is active.

Example

```
Dell#show snmp group

groupname: ngroup          security model: v3 auth
readview : nview          writeview: no write view specified
notifyview: nview
row status: active

Dell#
```

Related Commands

[snmp-server group](#) — configures an SNMP server group.

show snmp user

Display the information configured on each SNMP user name.

Z9500

Syntax

```
show snmp user
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp user
  User name: vlv2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile      active
  Authentication Protocol: None
  Privacy Protocol: None

Dell#
```

snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

Z9500

Syntax

```
snmp ifmib ifalias long
```

Defaults

Interface description truncated beyond 63 characters.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
!----command run on host connected to switch:-----!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to
```

```
IF-MIB::ifAlias.134792448 = STRING:

!----command run on Force10 switch:-----!
Dell#snmp ifmib ifalias long

!----command run on server connected to switch:-----!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i
alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected
to Router2. This is a
port connected to Router2. This is a port connected to
Router2. This is a port
connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
```

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

Z9500

Syntax

```
snmp-server community community-name {ro | rw} [ipv6 ipv6-
access-list-name [ipv6 ipv6-access-list-name | access-list-name
| security-name name] | security-name name [ipv6 ipv6-access-
list-name | access-list-name | security-name name] | access-
list-name [ipv6 ipv6-access-list-name | access-list-name |
security-name name]]
```

To remove access to a community, use the `no snmp-server community community-string {ro | rw} [security-name name [access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]]` command.

Parameters

<i>community-name</i>	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword <code>ro</code> to specify read-only permission.
rw	Enter the keyword <code>rw</code> to specify read-write permission.
ipv6 access-list-name	(Optional) Enter the keyword <code>ipv6</code> then an IPv6 ACL name (a string up to 16 characters long).
security-name <i>name</i>	(Optional) Enter the keywords <code>security-name</code> then the security name as defined by the community MIB.
access-list-name	(Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following example configures a community named *public* that is mapped to the security named *guestuser* with Read Only (*ro*) permissions.

The *security-name* parameter maps the community string to an SNMPv3 user/ security name as defined by the community MIB.

If a community string is configured without a *security-name* (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with *ro* (read-only) permissions.
- `v1v2cwriteu/ v1v2cwriteg` — maps to a community with *rw* (read-write) permissions.

The *community-name* parameter indexes this command.

If you do not configure the `snmp-server community` command, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional *access-list-name*.

The command options *ipv6*, *security-name*, and *access-list-name* are recursive. In other words, each option can, in turn, accept any of the three options as a sub-option, and each of those sub-options can accept any of the three sub-options as a sub-option, and so forth. The second Example shows the creation of a standard IPv4 ACL called *snmp-ro-acl* and then assigning it to the SNMP community *guest*.



NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs, port rules are not valid for SNMP.

Example

```
Dell#config
Dell(conf)# snmp-server community public ro
Dell(conf)# snmp-server community public ro security-name
guestuser
Dell(conf)#
```

Example

```
Dell(conf)# ip access-list standard snmp-ro-acl
Dell(config-std-nacl)#seq 5 permit host 10.10.10.224
Dell(config-std-nacl)#seq 10 deny any count
!

Dell(conf)#snmp-server community guest ro snmp-ro-acl
Dell(conf)#
```

Related Commands

[ip access-list standard](#) — names (or selects) a standard access list to filter based on IP address.

[ipv6 access-list](#) — configures an access list based on IPv6 addresses or protocols.

[show running-config](#) — displays the current SNMP configuration and defaults.

snmp-server contact

Configure contact information for troubleshooting this SNMP node.

Z9500

Syntax

```
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

Parameters

text Enter an alphanumeric text string, up to 55 characters long.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

snmp-server enable traps

Enable SNMP traps.

Z9500

Syntax

```
snmp-server enable traps [notification-type] [notification-option]
```

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.

Parameters

notification-type

Enter the type of notification from the following list:

- `bgp` — Enable notification of changes in the BGP process.
- `config` — Enable notification of changes to startup or running configuration.
- `ecfm` — Enable notification of changes to ECFM.
- `ecmp` — Enable notification of traffic imbalance in ECMP or a link bundle.
- `entity` — Enable notification of Entity Management Information Base (MIB) changes.
- `envmon` — Enable notification when an environmental threshold is exceeded.
- `hg-lbm` — Enable notification of hiGig link-bundle state changes.
- `isis` — Enable notification of IS-IS adjacency state changes.
- `lACP` — Enable notification of LACP state changes.
- `snmp` — Enable SNMP notifications defined in RFC 1157.
- `stp` — Enable notification of a state change in the spanning tree protocol (RFC 1493).
- `vlt` — Enable notification of VLT state changes.
- `vrrp` — Enable notification of a state change in a VRRP group.
- `xstp` — Enable notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.

notification-option

For the `envmon` notification-type, enter one of the following optional parameters:

- `cam-utilization`
- `fan`
- `supply`
- `temperature`

For the `snmp` notification-type, enter one of the following optional parameters:

- authentication
- coldstart
- linkdown
- linkup

Defaults Not enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for copy-config and ecmp traps.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for VRRP traps.
7.6.1.0	Added support for STP and xSTP traps. Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The system supports up to 16 SNMP trap receivers.

For the `cam-utilization` notification option, the system generates syslogs and SNMP traps when the L3 host table or route table utilization goes above the threshold.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

Related Commands [snmp-server community](#) — enables SNMP and sets the community string.
[snmp-server host](#) — configures an SNMP trap receiver.

snmp-server engineID

Configure the name for both the local and remote SNMP engines on the router.

Z9500

Syntax

```
snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]
```

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]` command.

Parameters	local engineID	Enter the keyword <code>local</code> followed by the engine ID number that identifies the copy of the SNMP on the local device. Format (as specified in RFC 3411): 12 octets. • The first four octets are set to the private enterprise number. • The remaining eight octets are the MAC address of the chassis.
	remote ip-address	Enter the keyword <code>remote</code> followed by the IP address that identifies the copy of the SNMP on the remote device.
	udp-port port-number engineID	Enter the keywords <code>udp-port</code> followed by the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is 162 .

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

Changing the value of the SNMP Engine ID has important side effects. A user's password (entered on the command line) is converted to a message digest algorithm (MD5) or secure hash algorithm (SHA) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users is invalid and the users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands

[show snmp engineID](#) — displays the SNMP engine and all the remote engines that are configured on the router.

[show running-config snmp](#) — displays the SNMP running configuration.

snmp-server group

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

Z9500

Syntax

```
snmp-server group [group_name {1 | 2c | 3 {auth | noauth |
priv}}} [read name] [write name] [notify name] [access access-
list-name | ipv6 access-list-name | access-list-name ipv6
access-list-name]]
```

To remove a specified group, use the `no snmp-server group [group_name {v1 | v2c | v3 {auth | noauth | priv}}} [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]]` command.

Parameters

group_name

Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults):

- `v1v2creadg` — maps to a community/security-name with `ro` permissions.
- `1v2cwriteg` — maps to a community/security-name `rw` permissions.

1 | 2c | 3

(OPTIONAL) Enter the security model version number (1, 2c, or 3):

- 1 is the least secure version.
- 3 is the most secure of the security modes.
- 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

The default is **1**.

auth	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.
read <i>name</i>	(OPTIONAL) Enter the keyword <code>read</code> then a name (a string of up to 20 characters long) as the read view name. The default is GlobalView and is assumed to be every object belonging to the internet (1.3.6.1) OID space.
write <i>name</i>	(OPTIONAL) Enter the keyword <code>write</code> then a name (a string of up to 20 characters long) as the write view name.
notify <i>name</i>	(OPTIONAL) Enter the keyword <code>notify</code> then a name (a string of up to 20 characters long) as the notify view name.
access <i>access-list-name</i>	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 <i>access-list-name</i>	(Optional) Enter the keyword <code>ipv6</code> then the IPv6 access list name (a string up to 16 characters long).
<i>access-list-name</i> <code>ipv6</code> <i>access-list-name</i>	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults

As above.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.2	Added support for the <code>access</code> parameter.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The following Example specifies the group named *harig* as a version 3 user requiring both authentication and encryption and read access limited to the read named *rview*.

 **NOTE:** The number of configurable groups is limited to 16 groups.

Example

```
Dell#conf
Dell(conf)# snmp-server group harig 3 priv read rview
Dell#
```

Related Commands [show snmp group](#) — displays the group name, security model, view status, and storage type of each group.

[show running-config](#) — displays the SNMP running configuration.

snmp-server host

Configure the recipient of an SNMP trap operation.

Z9500

Syntax

```
snmp-server host ip-address | ipv6-address [traps | informs]
[version 1 | 2c | 3] [auth | no auth | priv] [community-string]
[udp-port port-number] [notification-type]
```

To remove the SNMP host, use the `no snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

Parameters

ip-address Enter the keyword `host` then the IP address of the host (configurable hosts is limited to 16).

ipv6-address Enter the keyword `host` then the IPv6 address of the host in the x:x:x:x::x format.

 **NOTE:** The `::` notation specifies successive hexadecimal fields of zero.

traps (OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. The default is **traps**.

informs (OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. The default is **traps**.

version 1 | 2c | 3 (OPTIONAL) Enter the keyword `version` to specify the security model then the security model version number 1, 2c, or 3:

- Version 1 is the least secure version.
- Version 3 is the most secure of the security modes.

- Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

The default is version **1**.

auth	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community.



NOTE: For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking recommends setting the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.

udp-port port-number	(OPTIONAL) Enter the keywords <code>udp-port</code> followed by the port number of the remote host to use. The range is from 0 to 65535. The default is 162 .
notification-type	(OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host:

- `bgp` — BGP state change.
- `config` — copy—configuration traps.
- `ecfm` — ECFM state change.
- `ecmp` — ecmp and link bundling traffic imbalance traps.
- `entity` — Entity state change.
- `envmon` — Environment monitor trap.
- `hg-lbm` — HiGig link bundle state change.
- `isis` — ISIS adjacency state change.
- `lACP` — LACP state change.
- `snmp` — SNMP notification (RFC 1157).
- `vlt` — VLT state change.
- `stp` — Spanning tree protocol notification (RFC 1493).
- `vrrp` — State change in a VRRP group.
- `xstp` — State change in MSTP (802.1s), RSTP (802.1w), and PVST+.

The default is all trap types are sent to host.

Defaults	As above.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for config and ecmp traps.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for VRRP traps.
7.6.1.0	Added support for STP and xSTP notification types. Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information	In order to configure the router to send SNMP notifications, enter at least one <code>snmp-server host</code> command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an <code>snmp-server host</code> command, no notifications are sent. In order to enable multiple hosts, issue a separate <code>snmp-server host</code> command for each host. You can specify multiple notification types in the command for each host. When multiple <code>snmp-server host</code> commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last <code>snmp-server host</code> command will be in effect. For example, if you enter an <code>snmp-server host inform</code> command for a host and then enter another <code>snmp-server host inform</code> command for the same host, the second command replaces the first command. The <code>snmp-server host</code> command is used with the <code>snmp-server enable</code> command. Use the <code>snmp-server enable</code> command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one <code>snmp-server enable</code> command and the <code>snmp-server host</code> command for that host must be enabled.
--------------------------	--



NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

Related Commands

[snmp-server enable traps](#) — enables SNMP traps.

[snmp-server community](#) — configures a new community SNMPv1 or SNMPv2c.

snmp-server location

Configure the location of the SNMP server.

Z9500

Syntax

```
snmp-server location text
```

To delete the SNMP location, use the `no snmp-server location` command.

Parameters

text

Enter an alpha-numeric text string, up to 55 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell(config)#snmp-server location MAA_LAB
Dell(config)#do show running-config snmp
!
snmp-server community public ro
snmp-server location MAA_LAB
```

Related Commands

[show running-config snmp](#) — displays the SNMP running configuration.

snmp-server packetsize

Set the largest SNMP packet size permitted. When the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize global` configuration command.

Z9500

Syntax

```
snmp-server packetsize byte-count
```

Parameters

byte-count Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.

Defaults

8

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

Z9500

Syntax	<code>snmp-server trap-source <i>interface</i></code> To disable sending traps out a specific interface, use the <code>no snmp trap-source</code> command.																	
Parameters	<i>interface</i>	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.																
Defaults	The IP address assigned to the management interface is the default.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.5.1.0</td><td>Added support for 4-port 40G line cards on ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
Usage Information	To enable this <code>snmp-server trap-source</code> command, configure an IP address on the interface and enable the interface configured as an SNMP trap source.																	
Related Commands	snmp-server community — sets the community string.																	

snmp-server user

Configure a new user to an SNMP group.

Z9500

Syntax

```
snmp-server user name {group_name remote ip-address udp-port  
port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-  
password] [priv des56 priv password] [access access-list-name |  
ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]` command.

Parameters

name	Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.
group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • <code>v1v2creadu</code> — maps to a community with <code>ro</code> permissions. • <code>1v2cwriteu</code> — maps to a community <code>rw</code> permissions.
remote ip-address	Enter the keywords <code>udp-port</code> then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is 162 .
udp-port port-number	Enter the keywords <code>udp-port</code> then the UDP (User Datagram Protocol) port number on the remote device. The range is from 0 to 65535. The default is 162 .
1 2c 3	(OPTIONAL) Enter the security model version number (1, 2c, or 3): • 1 is the least secure version. • 3 is the most secure of the security modes. • 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is 1.
encrypted	(OPTIONAL) Enter the keyword <code>encrypted</code> to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.

	md5 sha (OPTIONAL) Enter the keyword <code>md5</code> or <code>sha</code> to designate the authentication level. • <code>md5</code> — Message Digest Algorithm • <code>sha</code> — Secure Hash Algorithm
	auth-password (OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host. Minimum: eight characters long.
	priv des56 (OPTIONAL) Enter the keywords <code>priv des56</code> to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (des56).
	priv password (OPTIONAL) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent. Minimum: eight characters long.
	access access-list-name (Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
	ipv6 access-list-name (Optional) Enter the keyword <code>ipv6</code> then the IPv6 access list name (a string up to 16 characters long).
	access-list-name ipv6 access-list-name (Optional) Enter both an IPv4 and IPv6 access list name.
Defaults	As above.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information



NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP. TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

No default values exist for authentication or privacy algorithms and no default password exists. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password is stored in the configuration in an encrypted form and displayed as encrypted in the `show running-config` command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an Example of how to specify the command with an encrypted string.



NOTE: The number of configurable users is limited to 16.

Example

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des56
d0452401a8c3ce42804fe80e3ba8763d
```

Usage Information

The following command is an example of how to enter a plain-text password as the string `authpasswd` for user `authuser` of group `v3group`.

Example

```
Dell#conf
Dell(conf)# snmp-server user authuser v3group v3 auth md5
authpasswd
```

Usage Information

The following command configures a remote user named `n3user` with a `v3` security model and a security level of `authNOPriv`.

Example

```
Dell#conf
Dell(conf)# snmp-server user n3user ngroup remote 172.31.1.3
udp-port 5009 3
auth md5 authpasswd
```

Related Commands

[show snmp user](#) — displays the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

Z9500

Syntax

```
snmp-server view view-name oid-tree {included | excluded}
```

To remove an SNMPv3 view, use the `no snmp-server view view-name oid-tree {included | excluded}` command.

Parameters

view-name

Enter the name of the view (not to exceed 20 characters).

	<i>oid-tree</i>	Enter the OID sub tree for the view (not to exceed 20 characters).														
	included	(OPTIONAL) Enter the keyword <code>included</code> to include the MIB family in the view.														
	excluded	(OPTIONAL) Enter the keyword <code>excluded</code> to exclude the MIB family in the view.														
Defaults	none															
Command Modes	CONFIGURATION															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.19.0	Introduced on the S4820T.															
8.3.11.1	Introduced on the Z9000.															
8.3.7.0	Introduced on the S4810.															
7.6.1.0	Introduced on the S-Series.															
7.5.1.0	Introduced on the C-Series.															
Usage Information	The <code>oid-tree</code> variable is a full sub-tree starting from 1.3.6 and cannot specify the name of a sub-tree or a MIB. The following Example configures a view named <code>rview</code> that allows access to all objects under 1.3.6.1.															
Example	<pre>Dell# conf Dell#(conf) snmp-server view rview 1.3.6.1 included</pre>															
Related Commands	show running-config snmp — displays the SNMP running configuration.															

snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

Z9500

Syntax	<pre>snmp trap link-status</pre> To disable sending link trap messages, use the <code>no snmp trap link-status</code> command.
Defaults	Enabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information If the interface is expected to flap during normal usage, you could disable this command.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

clear logging

Clear the messages in the logging buffer.

Z9500

Syntax `clear logging`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands [show logging](#) — displays logging settings and system messages in the internal buffer.

clear logging auditlog

Clears audit log.

Syntax	<code>clear logging auditlog</code>
Defaults	none
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Example `Dell(conf)#clear logging auditlog`

Related Commands [show logging auditlog](#) — displays audit log

default logging buffered

Return to the default setting for messages logged to the internal buffer.

Z9500

Syntax	<code>default logging buffered</code>
Defaults	size = 40960; level = 7 or debugging
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands [logging buffered](#) — sets the logging buffered parameters.

default logging console

Return the default settings for messages logged to the console.

Z9500

Syntax `default logging console`

Defaults **level = 7 or debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands [logging console](#) — sets the logging console parameters.

default logging monitor

Return to the default settings for messages logged to the terminal.

Z9500

Syntax `default logging monitor`

Defaults **level = 7 or debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands [logging monitor](#) — sets the logging monitor parameters.

[terminal monitor](#) — sends system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

Z9500

Syntax `default logging trap`

Defaults **level = 6 or informational**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands

[logging trap](#) — limit messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages are sent. Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Z9500

Syntax

```
logging {ip-address | ipv6-address | hostname} {{udp {port}} | {tcp {port}}}
```

To disable logging, use the `no logging {ip-address | ipv6-address | hostname} {port}` command.

Parameters

ip-address Enter the IPv4 address in dotted decimal format.

ipv6-address Enter the IPv6 address in the x:x:x:x::X format.



NOTE: The :: notation specifies successive hexadecimal fields of zeros.

hostname Enter the name of a host already configured and recognized by the switch.

udp Enter the keyword `udp` to enable transmission of log message over UDP followed by port number. The default port is 514

tcp Enter the keyword `tcp` to enable transmission of log message over TCP followed by port number.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added udp and tcp keywords for the Z9500.
9.5(0.0)	Added udp and tcp keywords for the S4810, S4820T, S6000, Z9000, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for IPv6.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Related Commands

[logging on](#) — enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.

[logging trap](#) — enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Z9500

Syntax

```
logging buffered [level] [size]
```

To return to the default values, use the default `logging buffered` command.

To disable logging stored to an internal buffer, use the `no logging buffered` command.

Parameters

<i>level</i>	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 7 or debugging .
<i>size</i>	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is from 40960 to 524288. The default is 40960 bytes .

Defaults	level = 7 ; size = 40960 bytes														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Usage Information	When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.														
Related Commands	clear logging — clears the logging buffer. default logging buffered — returns the logging buffered parameters to the default setting. show logging — displays the logging setting and system messages in the internal buffer.														

logging console

Specify which messages are logged to the console.

Z9500

Syntax	<pre>logging console [level]</pre> To return to the default values, use the <code>default logging console</code> command. To disable logging to the console, use the <code>no logging console</code> command.
Parameters	level (OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 7 or debugging.
Defaults	level = 7 ; size = debugging

Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Related Commands	clear logging — clears the logging buffer. default logging console — returns the logging console parameters to the default setting. show logging — displays the logging setting and system messages in the internal buffer.														

logging extended

Logs security and audit events to a system log server.

Syntax	<code>logging extended</code>						
Defaults	none						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.5(0.0)</td><td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.						

**Usage
Information**

This command is available with or without RBAC enabled. When RBAC is enabled you can restrict access to audit and security logs based on the CLI sessions' user roles. If extended logging is disabled, you can only view system events, regardless of RBAC user role.

When you enabled RBAC and extended logging:

- Only the system administrator role can execute this command.
- The system administrator and system security administrator roles can view security events and system events.
- The system administrator role can view audit, security, and system events.
- The network administrator and network operator roles can view system events.

Examples

```
Dell(conf)#logging extended
```

**Related
Commands**

[show logging auditlog](#) — displays audit log
[clear logging auditlog](#) — clears audit log

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

Z9500

Syntax

```
logging facility [facility-type]
```

To return to the default values, use the `no logging facility` command.

Parameters

facility-type

(OPTIONAL) Enter one of the following parameters:

- `auth` (authorization system)
- `cron` (Cron/at facility)
- `daemon` (system daemons)
- `kern` (kernel)
- `local0` (local use)
- `local1` (local use)
- `local2` (local use)
- `local3` (local use)
- `local4` (local use)
- `local5` (local use)
- `local6` (local use)
- `local7` (local use)
- `lpr` (line printer system)
- `mail` (mail system)
- `news` (USENET news)

- `sys9` (system use)
- `sys10` (system use)
- `sys11` (system use)
- `sys12` (system use)
- `sys13` (system use)
- `sys14` (system use)
- `syslog` (Syslog process)
- `user` (user process)
- `uucp` (Unix to Unix copy process)

The default is **local7**.

Defaults	local7														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Related Commands	logging — enables logging to a Syslog server. logging on — enables logging.														

logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

Z9500

Syntax	<pre>logging history level</pre> To return to the default values, use the <code>no logging history</code> command.
--------	---

Parameters	level Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 4 or warnings.														
Defaults	warnings or 4														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Usage Information	When you configure the <code>snmp-server trap-source</code> command, the system messages logged to the history table are also sent to the SNMP network management station.														
Related Commands	show logging — displays information logged to the history buffer.														

logging history size

Specify the number of messages stored in the logging history table.

Z9500

Syntax	<pre>logging history size size</pre> To return to the default values, use the <code>no logging history size</code> command.
Parameters	size Indicate a value as the number of messages to be stored. The range is from 0 to 500. The default is 1 message.
Defaults	1 message
Command Modes	CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

When the number of messages reach the limit you set with the `logging history size` command, older messages are deleted as newer ones are added to the table.

Related Commands

[show logging](#) — displays information logged to the history buffer.

logging monitor

Specify which messages are logged to Telnet applications.

Z9500

Syntax

```
logging monitor [level]
```

To disable logging to terminal connections, use the `no logging monitor` command.

Parameters

level Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults

7 or **debugging**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands [default logging monitor](#) — returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as the logging buffer, Syslog server, or terminal lines.

Z9500

Syntax `logging on`
To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

Defaults Enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information When you use the `no logging on` command, messages are logged only to the console.

Related Commands [logging](#) — enables logging to the Syslog server.

[logging buffered](#) — sets the logging buffered parameters.

[logging console](#) — sets the logging console parameters.

[logging monitor](#) — sets the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

Z9500

Syntax

`logging source-interface interface`

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For the management interface on the RPM, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
Usage Information	Syslog messages contain the IP address of the interface used to egress the router. By configuring the <code>logging source-interface</code> command, the Syslog packets contain the IP address of the interface configured.	
Related Commands	logging — enables logging to the Syslog server.	

logging synchronous

Synchronize unsolicited messages and output.

Z9500

Syntax	<pre>logging synchronous [level <i>level</i> all] [limit <i>number-of-buffers</i>]</pre> To disable message synchronization, use the <code>no logging synchronous [level <i>level</i> all] [limit <i>number-of-buffers</i>]</code> command.	
Parameters	all	Enter the keyword <code>all</code> to ensure that all levels are printed asynchronously.
	level <i>level</i>	Enter the keyword <code>level</code> then a number as the severity level. A high number indicates a low severity level and vice versa. The range is from 0 to 7. The default is 2 .
	all	Enter the keyword <code>all</code> to turn off all.
	limit <i>number-of-buffers</i>	Enter the keyword <code>limit</code> then the number of buffers to be queued for the terminal after which new messages are dropped. The range is from 20 to 300. The default is 20 .
Defaults	Disabled. If enabled without the <code>level</code> or <code>number-of-buffers</code> options specified, <code>level = 2</code> and <code>number-of-buffers = 20</code> are the defaults.	
Command Modes	LINE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
Usage Information	When you enable <code>logging synchronous</code>, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console. If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.														
Related Commands	logging on — enables logging.														
logging trap Specify which messages are logged to the Syslog server based the message severity. Z9500															
Syntax	<pre>logging trap [level]</pre> To return to the default values, use the default <code>logging trap</code> command. To disable logging, use the <code>no logging trap</code> command.														
Parameters	<table> <tr> <td><i>level</i></td><td>Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 6 or informational.</td></tr> </table>	<i>level</i>	Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 6 or informational .												
<i>level</i>	Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 6 or informational .														
Defaults	6 or informational														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.														

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series, S55.
7.5.1.0	Introduced on the C-Series.

Usage Information	To block a type of message parameter, set the logging trap level to a lower number. For example, to block severity messages at level 6, set the level to 5.
Related Commands	logging — enables the logging to another device. logging on — enables logging.

logging version

Displays syslog messages in a RFC 3164 or RFC 5424 format.

Syntax	<code>logging version {0 1}</code>						
Defaults	0						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.5(0.0)</td><td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.						

Usage Information	To display syslog messages in a RFC 3164 or RFC 5424 format, use the log version command in configuration mode. By default, the system log version is set to 0. The following describes the two supported log messages formats: 0 – Displays syslog messages format as described in RFC 3164, The BSD syslog Protocol 1 – Displays SYSLOG message format as described in RFC 5424, The Syslog Protocol
--------------------------	---

Example

```
Dell(conf)#logging version ?
<0-1> Select syslog version (default = 0)
Dell(conf)#logging version 1
```

show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

Z9500

Syntax

```
show logging [number | history [reverse][number] | reverse
[number] | summary]
```

Parameters

<i>number</i>	(OPTIONAL) Enter the number of messages displayed in the output. The range is from 1 to 65535.
<i>history</i>	(OPTIONAL) Enter the keyword <i>history</i> to view only information in the Syslog history table.
<i>reverse</i>	(OPTIONAL) Enter the keyword <i>reverse</i> to view the Syslog messages in FIFO (first in, first out) order.
<i>summary</i>	(OPTIONAL) Enter the keyword <i>summary</i> to view a table showing the number of messages per type and per slot. Slots *7* and *8* represent RPMs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example (Partial)

```
Dell#show logging

Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 97 Messages Logged, Size
(40960 bytes)
```



```

Trap logging: level informational
  Logging to 172.16.1.162
  Logging to 10.10.10.4
  Logging to 10.1.2.4
  Logging to 172.31.1.4
  Logging to 133.33.33.4
Feb 18 01:17:32: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:31: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed
interface Admin state to down: Fo 2/0
Feb 18 01:17:24: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:23: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:03: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
vty0 ( 10.16.127.145 )by admin
Feb 18 01:17:03: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed
interface Admin state to up: Fo 2/0
Feb 18 01:16:57: %SYSTEM:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.16.127.145 )
Feb 18 01:16:57: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on line vty0 ( 10.16.127.145 )
Feb 18 00:46:18: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty0 ( 10.16.127.145 )
Feb 18 00:46:17: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
vty0 ( 10.16.127.145 )by admin
- repeated 11 times
Feb 18 00:46:17: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed
interface Admin state to down: Fo 2/0
Feb 18 00:45:46: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
vty0 ( 10.16.127.145 )by admin
- repeated 6 times
Feb 18 00:45:46: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed
interface Admin state to up: Fo 2/0
Feb 18 00:45:40: %SYSTEM:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.16.127.145 )
Feb 18 00:45:40: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on line vty0 ( 10.16.127.145 )
Feb 18 00:43:10: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty0 ( 10.16.127.145 )
Feb 18 00:43:10: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed
interface Admin state to down: Fo 2/0
Feb 18 00:43:07: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
vty0 ( 10.16.127.145 )by admin
- repeated 6 times
Feb 18 00:42:44: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
vty0 ( 10.16.127.145 )by admin
Feb 18 00:42:44: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed
interface Admin state to up: Fo 2/0
Feb 18 00:42:38: %SYSTEM:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.16.127.145 )
Feb 18 00:42:38: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login
successful for user admin on line vty0 ( 10.16.127.145 )
Feb 18 00:39:38: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from
console
--More--

```

Example (History)

```

Dell#show logging history

Syslog History Table: 1 maximum table entries,

```

```
saving level warnings or higher
SNMP notifications not Enabled
Feb 18 01:16:57: %SYSTEM:CP %SEC-3-
AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication
success on vty0 ( 10.16.127.145 )
```

show logging auditlog

Displays an audit log.

Syntax	show logging auditlog						
Defaults	none						
Command Modes	EXEC						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.5(0.0)</td><td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL.</td></tr></tbody></table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.						
Example	Dell(conf)#show logging audit						
Related Commands	clear logging auditlog — clears audit log.						

show logging driverlog

Display the driver log for the specified hardware component.

Z9500

Syntax	show logging driverlog {cp rp linecard slot-id}	
Parameters	cp	Enter the keyword <code>cp</code> to display the driver log for the Control Processor on the switch.
	rp	Enter the keyword <code>rp</code> to display the driver log for the Route Processor on the switch.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify the line-card ports for which you want to display the driver log. The range of line-card slot IDs is from 0 to 2.
defaults	none	

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Examples

```
Dell# show logging driverlog cp
0:Task(dlm): [ 6472921]EEPROM LIB ERR: decipherPpId:349 PPID
ERROR: Mismatching VID and MFGID
```

```
1:Task(dlm): [ 101]EEPROM LIB ERR: decipherPpId:379
Invalid svcTag(n/a)
2:Task(dlm): [ 93]EEPROM LIB ERR: decipherPpId:390
strtoull invalidates svcTag(n/a): errno(0), *enr(/)
3:Task(dlm): [ 40]EEPROM LIB ERR: decipherPpId:416
svcTag invalid changing it to NA
4:Task(chmgr): [ 1555744]EEPROM LIB ERR: decipherPpId:349
PPID ERROR: Mismatching VID and MFGID
5:Task(chmgr): [ 50]EEPROM LIB ERR: decipherPpId:379
Invalid svcTag(n/a)
6:Task(chmgr): [ 42]EEPROM LIB ERR: decipherPpId:390
strtoull invalidates svcTag(n/a): errno(0), *ptr(/)
7:Task(chmgr): [ 39]EEPROM LIB ERR: decipherPpId:416
svcTag invalid changing it to NA
```

```
Dell# show logging driverlog linecard 0
```

```
0:Task(tUsrRoot): [ 29525]SS DRV DEBUG: Wrapper init
complete
1:Task(tUsrRoot): [ 301305]SS DRV DEBUG: Core init complete
2:Task(tUsrRoot): [ 913]SS DRV DEBUG: port:0 isfanout:0
3:Task(tUsrRoot): [ 40]SS DRV DEBUG: port:4 isfanout:0
4:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:8 isfanout:0
5:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:12 isfanout:0
6:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:16 isfanout:0
7:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:20 isfanout:0
8:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:24 isfanout:0
9:Task(tUsrRoot): [ 36]SS DRV DEBUG: port:28 isfanout:0
10:Task(tUsrRoot): [ 35]SS DRV DEBUG: port:32 isfanout:0
```

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

show logging kernellog

Display the kernel log for the specified hardware component.

Z9500

Syntax	show logging kernellog {cp rp linecard slot-id}	
Parameters	cp	Enter the keyword <code>cp</code> to display the kernel log for the Control Processor on the switch.
	rp	Enter the keyword <code>rp</code> to display the kernel log for the Route Processor on the switch.
	linecard slot-id	Enter the <code>linecard slot-id</code> parameters to specify the line-card ports for which you want to display the kernel log. The range of line-card slot IDs is from 0 to 2.
defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Examples	<pre>Dell# show logging kernellog cp 00:00:02:326592:AHCI_P_SCTL(0x01ac) 0x000000300 00:00:02:326599:AHCI_P_SERR(0x01b0) 0x000000000 00:00:02:326605:AHCI_P_SACT(0x01b4) 0x000000000 00:00:02:655656:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20 cmd_reg=0x8 rv=5 00:00:02:656982:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20 cmd_reg=0x9 rv=5 00:00:02:659597:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20 cmd_reg=0xf rv=5 00:00:43:418634:PCI unit 0: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver BCM56850_A0 00:00:43:418655:PCI unit 1: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver BCM56850_A0 00:00:43:418671:PCI unit 2: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver BCM56850_A0</pre>
----------	--

```

00:00:43:418687:PCI unit 3: Dev 0xb852, Rev 0x03, Chip
BCM56852_A2, Driver BCM56850_A0
00:00:43:418702:PCI unit 4: Dev 0xb852, Rev 0x03, Chip
BCM56852_A2, Driver BCM56850_A0
00:00:43:418718:PCI unit 5: Dev 0xb852, Rev 0x03, Chip
BCM56852_A2, Driver BCM56850_A0
00:00:43:418732:PCI unit 6: Dev 0xb636, Rev 0x11, Chip
BCM56636_B0, Driver BCM56634_B0

Dell#show logging kernellog rp
00:00:01:918834:ahcisata0 port 0: device present, speed:
6.0Gb/s
00:00:02:919154:ahcisata0 port 1: device not present
00:00:02:919164:
AHCI Global register dump
00:00:02:919171:AHCI_CAP(0x0000)          0xe237ff21
00:00:02:919178:AHCI_GHC(0x0004)          0x80000002
00:00:02:919184:AHCI_IS(0x0008) 0x00000000
00:00:02:919190:AHCI_PI(0x000c) 0x00000003
00:00:02:919197:AHCI_VS(0x0010) 0x00010000
00:00:02:919204:AHCI_CC_CTL(0x0014)        0x00010120
00:00:02:919210:AHCI_CC_PORTS(0x0018)      0x00000000
00:00:02:919217:AHCI_EM_LOC(0x001c)        0x00000000
00:00:02:919223:AHCI_EM_CTL(0x0020)        0x00000000
00:00:02:919229:AHCI per port register dump for port 1
00:00:02:919236:AHCI_P_IS(0x0190)          0x00000000
00:00:02:919243:AHCI_P_IE(0x0194)          0x00000000
00:00:02:919249:AHCI_P_CLBU(0x0184)        0x00000000
00:00:02:919255:AHCI_P_CLB(0x0180)         0x06491400
00:00:02:919262:AHCI_P_FBU(0x018c)         0x00000000
00:00:02:919269:AHCI_P_FB(0x0188)         0x06491900
00:00:02:919275:AHCI_P_CMD(0x0198)         0x00700016
00:00:02:919282:AHCI_P_CI(0x01b8)         0x00000000
00:00:02:919288:AHCI_P_TFD(0x01a0)         0x0000007f
00:00:02:919295:AHCI_P_SIG(0x01a4)         0xffffffff
00:00:02:919302:AHCI_P_SSTS(0x01a8)        0x00000000
00:00:02:919308:AHCI_P_SCTL(0x01ac)        0x00000300
00:00:02:919315:AHCI_P_SERR(0x01b0)       0x00000000
00:00:02:919321:AHCI_P_SACT(0x01b4)       0x00000000

Dell#show logging kernellog linecard 0
1d 02:24:49:841597:qsfp-3 eeprom attempting to read on from
iic at : 14
1d 02:24:49:849249:qsfp-6 eeprom attempting to read on from
iic at : 24
1d 02:24:49:856820:qsfp-7 eeprom attempting to read on from
iic at : 23
1d 02:24:49:872175:qsfp-11 eeprom attempting to read on from
iic at : 18
1d 02:26:50:140882:qsfp-0 eeprom attempting to read on from
iic at : 17
1d 02:26:50:148668:qsfp-1 eeprom attempting to read on from
iic at : 16
1d 02:26:50:156237:qsfp-2 eeprom attempting to read on from
iic at : 15
1d 02:26:50:163966:qsfp-3 eeprom attempting to read on from
iic at : 14
1d 02:26:50:179846:qsfp-6 eeprom attempting to read on from
iic at : 24
1d 02:26:50:187498:qsfp-7 eeprom attempting to read on from
iic at : 23
1d 02:26:50:202989:qsfp-11 eeprom attempting to read on from
iic at : 18
1d 02:28:50:440146:qsfp-0 eeprom attempting to read on from

```

```
iic at : 17
1d 02:28:50:447933:qsfp-1 eeprom attempting to read on from
iic at : 16
1d 02:28:50:455505:qsfp-2 eeprom attempting to read on from
iic at : 15
1d 02:28:50:463233:qsfp-3 eeprom attempting to read on from
iic at : 14
1d 02:28:50:470881:qsfp-6 eeprom attempting to read on from
iic at : 24
1d 02:28:50:478591:qsfp-7 eeprom attempting to read on from
iic at : 23
1d 02:28:50:493790:qsfp-11 eeprom attempting to read on from
iic at : 18
1d 02:30:50:675435:qsfp-0 eeprom attempting to read on from
iic at : 17
1d 02:30:50:683019:qsfp-1 eeprom attempting to read on from
iic at : 16
```

Usage Information This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed port pipe.

terminal monitor

Configure the system to display messages on the monitor/terminal.

Z9500

Syntax `terminal monitor`
To return to default settings, use the `terminal no monitor` command.

defaults Disabled.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

**Related
Commands**

[logging monitor](#) — sets the logging parameters on the monitor/terminal.

SNMP Traps

This chapter lists the traps sent by the Dell Networking operating system. Each trap is listed by the fields Message ID, Trap Type, and Trap Option.

Message ID	Trap Type	Trap Option
COLD_START	SNMP	COLDSTART
%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.		
WARM_START	SNMP	WARMSTART
COPY_CONFIG_COMPLETE	SNMP	NONE
SNMP Copy Config Command Completed		
LINK_DOWN	SNMP	LINKDOWN
%IFA-1-PORT_LINKDN: changed interface state to down:%d		
LINK_UP	SNMP	LINKUP
%IFA-1-PORT_LINKUP: changed interface state to up: %d		
AUTHENTICATION_FAIL	SNMP	AUTH
%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.		
EGP_NEIGHBOR_LOSS	SNMP	NONE
OSTATE_DOWN	SNMP	LINKDOWN
%IFM-1-OSTATE_DN: changed interface state to down: %s		
%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s		
OSTATE_UP	SNMP	LINKUP
%IFM-1-OSTATE_UP: changed interface state to up:%s		
%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s		
RMON_RISING_THRESHOLD	SNMP	NONE
%SYSTEM-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>		
RMON_FALLING_THRESHOLD	SNMP	NONE

Message ID	Trap Type	Trap Option
%SYSTEM-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>		
RMON_HC_RISHING_THRESHOLD	SNMP	NONE
%SYSTEM-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>		
RMON_HC_FALLING_THRESHOLD	SNMP	NONE
%SYSTEM-P:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>		
RESV	NONE	NONE
N/A		
CHM_CARD_DOWN	ENVMON	NONE
%CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s		
%CHMGR-2-CARD_DOWN: %sLine card %d down - %s		
CHM_CARD_UP	ENVMON	NONE
%CHMGR-5-LINECARDUP: %sLine card %d is up		
CHM_CARD_MISMATCH	ENVMON	NONE
%CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.		
CHM_CARD_PROBLEM	ENVMON	NONE
CHM_ALARM_CUTOFF	ENVMON	NONE
CHM_PWRSRC_DOWN	ENVMON	SUPPLY
%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s		
CHM_PWRSRC_CLR	ENVMON	SUPPLY
%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good		
CHM_MAJ_ALARM_PS	ENVMON	SUPPLY
%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s		
CHM_MAJ_ALARM_PS_CLR	ENVMON	SUPPLY
%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power		
CHM_MIN_ALARM_PS	ENVMON	SUPPLY
%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant		
CHM_MIN_ALARM_PS_CLR	ENVMON	SUPPLY

Message ID	Trap Type	Trap Option
%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant		
CHM_MIN_ALARM_TEMP	ENVMON	TEMP
%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature		
CHM_MIN_ALARM_TEMP_CLR	ENVMON	TEMP
%CHMGR-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)		
CHM_MAJ_ALARM_TEMP	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)		
CHM_MAJ_ALARM_TEMP_CLR	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)		
CHM_FANTRAY_BAD	ENVMON	FAN
%CHMGR-2-FAN_TRAY_BAD: Major alarm: fan tray %d is missing or down		
%CHMGR-2-ALL_FAN_BAD: Major alarm: all fans in fan tray %d are down.		
%CHMGR-2-FANTRAYBAD: Major alarm: fan tray is missing		
%CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down		
CHM_FANTRAY_BAD_CLR	ENVMON	FAN
%CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray %d present		
%CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present		
CHM_MIN_FANBAD	ENVMON	FAN
%CHMGR-2-FAN_BAD: Minor alarm: some fans in fan tray %d are down		
%CHMGR- 2-1FANBAD: Minor alarm: fan in fan tray is down		
CHM_MIN_FANBAD_CLR	ENVMON	FAN
%CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good		

Message ID	Trap Type	Trap Option
%CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good		
TME_TASK_SUSPEND	ENVMON	NONE
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
TME_TASK_TERM	ENVMON	NONE
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
CHM_CPU_THRESHOLD	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
CHM_CPU_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
CHM_MEM_THRESHOLD	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
CHM_MEM_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
MACMGR_STN_MOVE	ENVMON	NONE
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
VRRP_BADAUTH	PROTO	NONE
%SYSTEM-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Te 1/12 rcvd pkt with authentication type mismatch.		
%SYSTEM-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Te 1/12 rcvd pkt with authentication failure		
VRRP_GO_MASTER	PROTO	NONE
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		
VRRP_PROTOCOL_ERROR	PROTO	NONE
VRRP_PROTOERR: VRRP protocol error on %S		
BGP4_ESTABLISHED	PROTO	NONE
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
BGP4_BACKW_XSITION	PROTO	NONE
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		

Storm Control

The Dell Networking operating software storm control feature allows you to limit or suppress traffic during a traffic storm (Broadcast/Unknown Unicast Rate Limiting or Multicast on the C-Series and S-Series).

Important Points to Remember

- Interface commands can only be applied on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- You can apply the CONFIGURATION-level storm control commands at ingress or egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. It is not based on the speed setting for the line card.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).
- When you enable broadcast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic goes to queue 1 instead of queue 0.
- Similarly, if you enable unicast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic goes to queue 2 instead of queue 0.

 **NOTE:** Bi-directional traffic (unknown unicast and broadcast) along with egress storm control causes the configured traffic rates split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port pipes or the same/different line cards.

show storm-control broadcast

Display the storm control broadcast configuration.

Z9500

Syntax	<code>show storm-control broadcast [<i>interface</i>]</code>	
Parameters	<i>interface</i>	(OPTIONAL) Enter one of the following interfaces to display the interface-specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

show storm-control multicast

Display the storm control multicast configuration.

Z9500

Syntax `show storm-control multicast [interface]`

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell#show storm-control multicast tengigabitethernet 1/0

Multicast storm control configuration

Interface Direction Packets/Second
-----
Te 1/0      Ingress      5
```

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

Z9500

Syntax `show storm-control unknown-unicast [interface]`

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in the network.

Z9500

Syntax

```
storm-control broadcast [packets_per_second in]
```

To disable broadcast rate-limiting, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

<i>packets_per_second</i> in	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.
---	--

Defaults

none

Command Modes

CONFIGURATION (conf)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the percentage decimal value option.
6.5.1.0	Introduced on the E-Series.

Usage Information Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface (ingress only).

Z9500

Syntax `storm-control broadcast [packets_per_second in]`
To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

<i>packets_per_second in</i>	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.
-------------------------------------	--

Defaults none

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the <code>percentage decimal value</code> option.
6.5.1.0	Introduced on the E-Series.

storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic allowed into the C-Series and S-Series networks only.

Z9500

Syntax `storm-control multicast packets_per_second in`
To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.

Parameters

<i>packets_per_second</i> in	Enter the packets per second of multicast traffic allowed into the network. The range is from 0 to 33554368.
-------------------------------------	--

Defaults none

Command Modes CONFIGURATION (conf)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-series and S-Series.

Usage Information Broadcast traffic (all 0xFs) should be counted against the broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that

some multicast control traffic may get dropped when storm control thresholds are exceeded.

storm-control multicast (Interface)

Configure the percentage of multicast traffic allowed on an C-Series or S-Series interface (ingress only) network only.

Z9500

Syntax `storm-control multicast packets_per_second in`
To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

Parameters

<i>packets_per_second in</i>	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.
-------------------------------------	--

Defaults none

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-series and S-Series.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

Z9500

Syntax `storm-control unknown-unicast [packets_per_second in]`

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second in]` command.

Parameters

packets_per_second in Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the percentage decimal value option.
6.5.1.0	Introduced on the E-Series.

Usage

Information

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (ingress only).

Z9500

Syntax

```
storm-control unknown-unicast [percentage decimal_value in] |  
[wred-profile name]] [packets_per_second in]
```

To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]] [packets_per_second in]` command.

Parameters

percentage
decimal_value
[in | out]

E-Series Only: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%.

The percentage is from 0 to 100:

- 0% blocks all related traffic.
- 100% allows all traffic into the interface.

The decimal range is from 0.1 to 0.9.

wred-profile
name

E-Series Only: (Optionally) Enter the keywords *wred-profile* followed by the profile name to designate a wred-profile.

packets_per_second
cond in

C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554431.

Defaults

none

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the <i>percentage decimal value</i> option.
6.5.1.0	Introduced on the E-Series.

Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP).

bpdu-destination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Z9500

Syntax	bpdu-destination-mac-address [xstp gvrp] provider-bridge-group	
Parameters	xstp	Force STP, RSTP, and MSTP to use the Provider Bridge Group address as the destination MAC address in its BPDUs.
	gvrp	Forces GVRP to use the Provider Bridge GVRP Address as the destination MAC address in its PDUs.
Defaults	The destination MAC address for BPDUs is the Bridge Group Address.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

Z9500

Syntax	<code>bridge-priority {priority-value primary secondary}</code> To return to the default value, use the <code>no bridge-priority</code> command.	
Parameters	priority-value	Enter a number as the bridge priority value. The range is from 0 to 65535. The default is 32768 .
	primary	Enter the keyword <code>primary</code> to designate the bridge as the root bridge.
	secondary	Enter the keyword <code>secondary</code> to designate the bridge as a secondary root bridge.
Defaults	priority-value = 32768	
Command Modes	SPANNING TREE (The prompt is "config-stp".)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

Z9500

Syntax	<code>debug spanning-tree {stp-id [all bpdu config events exceptions general root] protocol}</code>
--------	---

To disable debugging, use the `no debug spanning-tree` command.

Parameters

<i>stp-id</i>	Enter zero (0). The switch supports one spanning tree group with a group ID of 0.
<i>protocol</i>	Enter the keyword for the type of STP to debug, either <code>mstp</code> , <code>pvst</code> , or <code>rstp</code> .
<i>all</i>	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
<i>bpdu</i>	(OPTIONAL) Enter the keyword <code>bpdu</code> to debug bridge protocol data units.
<i>config</i>	(OPTIONAL) Enter the keyword <code>config</code> to debug configuration information.
<i>events</i>	(OPTIONAL) Enter the keyword <code>events</code> to debug STP events.
<i>general</i>	(OPTIONAL) Enter the keyword <code>general</code> to debug general STP operations.
<i>root</i>	(OPTIONAL) Enter the keyword <code>root</code> to debug STP root transactions.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

Related Commands

[protocol spanning-tree](#) — enters SPANNING TREE mode on the switch.

description

Enter a description of the spanning tree.

Z9500

Syntax	<code>description {description}</code> To remove the description from the spanning tree, use the <code>no description {description}</code> command.													
Parameters	description	Enter a description to identify the spanning tree (80 characters maximum).												
Defaults	none													
Command Modes	SPANNING TREE (The prompt is "config-stp".)													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.0</td><td>Introduced</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Introduced
Version	Description													
9.2(1.0)	Introduced on the Z9500.													
8.3.19.0	Introduced on the S4820T.													
8.3.11.1	Introduced on the Z9000.													
8.3.7.0	Introduced on the S4810.													
7.7.1.0	Introduced													
Related Commands	protocol spanning-tree — enters SPANNING TREE mode on the switch.													

disable

Disable the spanning tree protocol globally on the switch.

Z9500

Syntax	<code>disable</code> To enable Spanning Tree Protocol, use the <code>no disable</code> command.
Defaults	Enabled (that is, the spanning tree protocol is disabled.)

Command Modes	SPANNING TREE																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.7.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.7.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																
Related Commands	protocol spanning-tree — enters SPANNING TREE mode on the switch.																

forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

Z9500

Syntax	<code>forward-delay seconds</code> To return to the default setting, use the <code>no forward-delay</code> command.	
Parameters	seconds	Enter the number of seconds the system waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is 15 seconds .
Defaults	15 seconds	
Command Modes	SPANNING TREE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

[max-age](#) — changes the wait time before STP refreshes protocol configuration information.

[hello-time](#) — changes the time interval between BPDUs.

hello-time

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

Z9500

Syntax

`hello-time seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds

Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

[forward-delay](#) — changes the wait time before STP transitions to the Forwarding state.

[max-age](#) — changes the wait time before STP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the spanning tree bridge.

Z9500

Syntax

`max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

seconds

Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

	Version	Description
	7.7.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.2.1.1	Introduced on the E-Series.
Related Commands	forward-delay — changes the wait time before STP transitions to the Forwarding state. hello-time — changes the time interval between BPDUs.	

protocol spanning-tree

To enable and configure the spanning tree group, enter SPANNING TREE mode.

Z9500

Syntax	<code>protocol spanning-tree stp-id</code> To disable the Spanning Tree group, use the <code>no protocol spanning-tree stp-id</code> command.	
Parameters	stp-id	Enter zero (0). the system supports one spanning tree group, group 0.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the <code>no disable</code> command from SPANNING TREE mode.
Example	<pre>Dell(config)#protocol spanning-tree 0 Dell(config-stp)#</pre>
Related Commands	disable — disables spanning tree group 0. To enable spanning tree group 0, use the <code>no disable</code> command.

show config

Display the current configuration for the mode. Only non-default values display.

Z9500

Syntax	<code>show config</code>
Command Modes	SPANNING TREE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example	<pre>Dell(config-stp)#show config protocol spanning-tree 0 no disable Dell(config-stp)#</pre>
----------------	---

show spanning-tree 0

Display the spanning tree group configuration and status of interfaces in the spanning tree group.

Z9500

Syntax	<code>show spanning-tree 0 [active brief guard interface interface root summary]</code>	
Parameters	0	Enter 0 (zero) to display information about that specific spanning tree group.
	active	(OPTIONAL) Enter the keyword <code>active</code> to display only active interfaces in spanning tree group 0.
	brief	(OPTIONAL) Enter the keyword <code>brief</code> to display a synopsis of the spanning tree group configuration information.
	guard	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an STP interface and the current port state.
	interface interface	(OPTIONAL) Enter the keyword <code>interface</code> and the type slot/port of the interface you want displayed. Type slot/port options are the following: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	root	(OPTIONAL) Enter the keyword <code>root</code> to display configuration information on the spanning tree group root.
	summary	(OPTIONAL) Enter the keyword <code>summary</code> to only the number of ports in the spanning tree group and their state.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.5.1.0	Added support for 4-port 40G line cards on the E-Series ExaScale.
8.4.2.1	Added support for the optional <code>guard</code> keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

Enable spanning tree group 0 prior to using this command.

The following describes the `show spanning-tree 0` command shown in the example.

Field	Description
"Bridge Identifier..."	Lists the bridge priority and the MAC address for this STP bridge.
"Configured hello..."	Displays the settings for hello time, max age, and forward delay.
"We are..."	States whether this bridge is the root bridge for the STG.
"Current root..."	Lists the bridge priority and MAC address for the root bridge.
"Topology flag..."	States whether the topology flag and the detected flag were set.
"Number of..."	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
"Timers"	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
"Times"	List the number of seconds since the last: • hello time • topology change • notification • aging
"Port 1..."	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
"Port path..."	Displays the path cost, priority, and identifier for the interface.
"Designated root..."	Displays the priority and MAC address of the root bridge of the STG that the interface belongs to.

Field	Description
"Designated port..."	Displays the designated port ID.

Example

```
Dell#show spanning-tree 0

Executing IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Current root has priority 32768 address 0001.e800.0a56
Topology change flag set, detected flag set
Number of topology changes 1 last change occurred 0:00:05 ago
  from TenGigabitEthernet 1/3
Timers:hold 1, topology change 35
      hello 2, max age 20, forward_delay 15
Times:hello 1, topology change 1, notification 0, aging 2

Port 26 (TenGigabitEthernet 1/1) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.26
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.26, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 27 (TenGigabitEthernet 1/2) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.27
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.27, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 28 (TenGigabitEthernet 1/3) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.28
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.28, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:31, received 0
The port is not in the portfast mode

Dell#
```

Example (Brief)

```
Dell#show span 0 brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768
      Address 0001.e800.0a56
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768,
      Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
Interface                               Designated
Name   PortID Prio Cost Sts Cost Bridge ID          PortID
```



```

-----
Te 1/1 8.26 8 4 FWD 0 32768 0001.e800.0a56 8.26
Te 1/2 8.27 8 4 FWD 0 32768 0001.e800.0a56 8.27
Te 1/3 8.28 8 4 FWD 0 32768 0001.e800.0a56 8.28
Dell#

```

Usage Information

The following describes the `show spanning-tree 0 guard` command shown in the example.

Field	Description
Interface Name	STP interface.
Instance	STP 0 instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```

Dell#show spanning-tree 0 guard
Interface
Name      Instance Sts              Guard type
-----
Te 0/1 0          INCON(Root)    Rootguard
Te 0/2 0          LIS           Loopguard
Te 0/3 0          EDS (Shut)    Bpduguard

```

spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

Z9500

Syntax

```

spanning-tree stp-id {cost cost | | portfast [bpduguard
[shutdown-on-violation]] | priority priority}

```

To disable Spanning Tree group on an interface, use the `no spanning-tree stp-id {cost cost | portfast [bpduguard [shutdown-on-violation]] | priority priority}` command.

Parameters

<i>stp-id</i>	Enter the STP instance ID. The range is 0.
<i>cost cost</i>	Enter the keyword <i>cost</i> then a number as the cost. The range is from 1 to 65535. The defaults are: 10-Gigabit Ethernet interface = 2. - Port Channel interface with 10-Gigabit Ethernet = 1.

portfast [bpduguard [shutdown-on-violation]]	Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the optional keyword <code>bpduguard</code> to disable the port when it receives a BPDU. Enter the optional keyword <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
priority <i>priority</i>	Enter keyword <code>priority</code> then a number as the priority. The range is from zero (0) to 15. The default is 8 .

Defaults

cost = depends on the interface type; priority = **8**

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.1	Introduced the <code>loopguard</code> and <code>rootguard</code> options on the S4810.
8.4.2.1	Introduced the <code>loopguard</code> and <code>rootguard</code> options on the E-Series TeraScale, C-Series, and S-Series.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the <code>shutdown-on-violation</code> option.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

If you enable `portfast bpduguard` on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in `ERR_DISABLE` mode, yet appears in the `show interface` commands as enabled. If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

STP loop guard and root guard are supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST+).

Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.

STP root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard.`

Do not enable Portfast BPDU guard and loop guard at the same time on a port. Enabling both features may result in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

To display the type of STP guard (Portfast BPDU, root, or loop guard) enabled on a port, enter the `show spanning-tree 0` command.

System Time and Date

The commands in this chapter configure time values on the system, either using the Dell Networking operating software, or the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host.

For more information, refer to the “Network Time Protocol” section of the *Management* chapter in the *Dell Networking OS Configuration Guide*.

calendar set

Set the time and date for the switch hardware clock.

Z9500

Syntax	<code>calendar set time month day year</code>	
Parameters	<i>time</i>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; for example, 17:15:00 is 5:15 pm.
	<i>month</i>	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
	<i>day</i>	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
	<i>year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

	Version	Description
	8.3.11.1	Introduced on the Z9000.
	8.3.7.0	Introduced on the S4810.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	6.1.1.0	Introduced on the E-Series.
Usage Information	You can change the order of the month and day parameters to enter the time and date as time day month year. In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the system automatically updates the software clock after system bootup. You cannot delete the hardware clock (calendar). To manually update the software with the hardware clock, use the <code>clock read-calendar</code> command.	
Example	<pre>Dell#calendar set 08:55:00 june 18 2006 Dell#</pre>	
Related Commands	clock read-calendar — sets the software clock based on the hardware clock. clock set — sets the software clock. show clock — displays the clock settings.	

clock read-calendar

Set the software clock on the switch from the information set in hardware clock (calendar).

Z9500

Syntax	<code>clock read-calendar</code>
Defaults	Not configured.
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the system automatically updates the software clock after system bootup.

You cannot delete this command (there is not a `no` version of this command).

clock set

Set the software clock in the switch.

Z9500

Syntax

```
clock set time month day year
```

Parameters

<i>time</i>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
<i>month</i>	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to time day month year.
<i>day</i>	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time month day year.
<i>year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

You can change the order of the `month` and `day` parameters to enter the time and date as time day month year. You cannot delete the software clock.

The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.

Dell Networking recommends using an outside time source, such as NTP, to ensure accurate time on the switch.

Example

```
Dell#clock set 16:20:00 19 may 2001
Dell#
```

Related Commands

[ntp update-calendar](#) — sets the switch using the NTP settings.

clock summer-time date

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

Z9500

Syntax

```
clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

<i>time-zone</i>	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
<i>start-month</i>	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.

<i>start-day</i>	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
<i>start-year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.
<i>start-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-day</i>	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
<i>end-month</i>	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
<i>end-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.
<i>offset</i>	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is 60 minutes .

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands [calendar set](#) — sets the hardware clock.

[clock summer-time recurring](#) — sets a date (and time zone) on which to convert the switch to daylight saving time each year.

[show clock](#) — displays the current clock settings.

clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

Z9500

Syntax

```
clock summer-time time-zone recurring [start-week start-day  
start-month start-time end-week end-day end-month end-time  
[offset]]
```

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

<i>time-zone</i>	Enter the three-letter name for the time zone. This name is displayed in the show clock output. You can enter up to eight characters.
<i>start-week</i>	(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for start-day through end-time: • week-number: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time. • first: Enter this keyword to start daylight saving time in the first week of the month. • last: Enter this keyword to start daylight saving time in the last week of the month.
<i>start-day</i>	Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations; for example, Sun, Sat, Mon, and so on. The range is from Sun to Sat.
<i>start-month</i>	Enter the name of one of the 12 months in English.
<i>start-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-week</i>	Enter the one of the following as the week that daylight saving ends: • week-number: enter a number from 1 to 4 as the number of the week to end daylight saving time. • first: enter the keyword <code>first</code> to end daylight saving time in the first week of the month. • last: enter the keyword <code>last</code> to end daylight saving time in the last week of the month.

<i>end-day</i>	Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations; for example Sun, Sat, Mon, and so on. The range is from Sun to Sat.
<i>end-month</i>	Enter the name of one of the 12 months in English.
<i>end-time</i>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
<i>offset</i>	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is 60 minutes .

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Updated the <code>start-day</code> and <code>end-day</code> options to allow for using the three-letter abbreviation of the weekday name.
6.1.1.0	Introduced on the E-Series.

Related Commands [calendar set](#) — sets the hardware clock.

[clock summer-time date](#) — sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

[show clock](#) — displays the current clock settings.

clock timezone

Configure a timezone for the switch.

Z9500

Syntax	<code>clock timezone <i>timezone-name</i> <i>offset</i></code> To delete a timezone configuration, use the <code>no clock timezone</code> command.																	
Parameters	<i>timezone-name</i>	Enter the name of the timezone. You cannot use spaces.																
	<i>offset</i>	Enter one of the following: - a number from 1 to 23 as the number of hours in addition to universal time coordinated (UTC) for the timezone. - a minus sign (-) then a number from 1 to 23 as the number of hours.																
Defaults	Not configured.																	
Command Modes	CONFIGURATION																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description																	
9.2(1.0)	Introduced on the Z9500.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.11.1	Introduced on the Z9000.																	
8.3.7.0	Introduced on the S4810.																	
7.6.1.0	Introduced on the S-Series.																	
7.5.1.0	Introduced on the C-Series.																	
6.1.1.0	Introduced on the E-Series.																	
Usage Information	Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.																	

debug ntp

Display network time protocol (NTP) transactions and protocol messages for troubleshooting.

Z9500

Syntax

```
debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}
```

To disable debugging of NTP transactions, use the `no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` command.

Parameters	adjust	Enter the keyword <code>adjust</code> to display information on NTP clock adjustments.
	all	Enter the keyword <code>all</code> to display information on all NTP transactions.
	authentication	Enter the keyword <code>authentication</code> to display information on NTP authentication transactions.
	events	Enter the keyword <code>events</code> to display information on NTP events.
	loopfilter	Enter the keyword <code>loopfilter</code> to display information on NTP local clock frequency.
	packets	Enter the keyword <code>packets</code> to display information on NTP packets.
	select	Enter the keyword <code>select</code> to display information on the NTP clock selection.
	sync	Enter the keyword <code>sync</code> to display information on the NTP clock synchronization.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

Z9500

Syntax	<code>ntp authenticate</code> To disable NTP authentication, use the <code>no ntp authentication</code> command.
Defaults	Not enabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information	You also must configure an authentication key for NTP traffic using the <code>ntp authentication-key</code> command.
Related Commands	ntp authentication-key — configures the authentication key for NTP traffic. ntp trusted-key — configures a key to authenticate.

ntp authentication-key

Specify a key for authenticating the NTP server.

Z9500

Syntax	ntp authentication-key <i>number</i> md5 [0 7] <i>key</i>															
Parameters	<i>number</i>	Specify a number for the authentication key. The range is from 1 to 4294967295. This number must be the same as the <i>number</i> parameter configured in the <i>ntp trusted-key</i> command.														
	md5	Specify that the authentication key is encrypted using MD5 encryption algorithm.														
	0	Specify that authentication key is entered in an unencrypted format (default).														
	7	Specify that the authentication key is entered in DES encrypted format.														
	<i>key</i>	Enter the authentication key in the previously specified format.														
Defaults	NTP authentication is not configured by default. If you do not specify the option [0 7], 0 is selected by default.															
Command Modes	CONFIGURATION															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.2.1.0</td><td>Added options [0 7] for entering the authentication key.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.2.1.0	Added options [0 7] for entering the authentication key.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description															
9.2(1.0)	Introduced on the Z9500.															
8.3.11.1	Introduced on the Z9000.															
8.2.1.0	Added options [0 7] for entering the authentication key.															
7.6.1.0	Introduced on the S-Series.															
7.5.1.0	Introduced on the C-Series.															
6.1.1.0	Introduced on the E-Series.															
Usage Information	After configuring the <i>ntp authentication-key</i> command, configure the <i>ntp trusted-key</i> command to complete NTP authentication. The Dell Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous versions; beginning in															

version 8.2.1.0, the system uses DES encryption to store the key in the startup-config when you enter the `ntp authentication-key` command. Therefore, if your system boots with a startup-configuration from a version prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

**Related
Commands**

[ntp authenticate](#) — enables NTP authentication.

[ntp trusted-key](#) — configures a trusted key.

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

Z9500

Syntax

`ntp broadcast client`

To disable broadcast, use the `no ntp broadcast client` command.

Defaults

Disabled.

**Command
Modes**

INTERFACE

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp disable

Prevent an interface from receiving NTP packets.

Z9500

Syntax	<code>ntp disable</code> To re-enable NTP on an interface, use the <code>no ntp disable</code> command.
Defaults	Disabled (that is, if you configure an NTP host, all interfaces receive NTP packets)
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp multicast client

To receive NTP information from the network via multicast, configure the switch.

Z9500

Syntax	<code>ntp multicast client [multicast-address]</code> To disable multicast reception, use the <code>no ntp multicast client [multicast-address]</code> command.		
Parameters	<table><tr><td><i>multicast-address</i></td><td>(OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in X:X:X:X::X format. If you do not enter a multicast address, the address:</td></tr></table>	<i>multicast-address</i>	(OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in X:X:X:X::X format. If you do not enter a multicast address, the address:
<i>multicast-address</i>	(OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in X:X:X:X::X format. If you do not enter a multicast address, the address:		

- 224.0.1.1 is configured if the interface address is IPv4
- ff05::101 is configured if the interface address is IPv6

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Added support for IPv6 multicast addresses.
8.3.7.0	Introduced on the S4810.
6.1.1.0	Introduced on the E-Series.

ntp server

Configure an NTP time-serving host.

Z9500

Syntax `ntp server {hostname | ipv4-address | ipv6-address} [key keyid] [prefer] [version number]`

Parameters	<i>ipv4-address</i> <i>ipv6-address</i>	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
	<i>hostname</i>	Enter the hostname of the server.
	<i>key keyid</i>	(OPTIONAL) Enter the keyword <code>key</code> and a number as the NTP peer key. The range is from 1 to 4294967295.
	<i>prefer</i>	(OPTIONAL) Enter the keyword <code>prefer</code> to indicate that this peer has priority over other servers.
	<i>version number</i>	(OPTIONAL) Enter the keyword <code>version</code> and a number to correspond to the NTP version used on the server. The range is from 1 to 3.

Defaults	Not configured.														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.4.1.0</td><td>Added IPv6 support.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.11.1	Introduced on the Z9000.	8.4.1.0	Added IPv6 support.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.11.1	Introduced on the Z9000.														
8.4.1.0	Added IPv6 support.														
7.6.1.0	Introduced on the S-Series.														
7.5.1.0	Introduced on the C-Series.														
6.1.1.0	Introduced on the E-Series.														
Usage Information	You can configure multiple time-serving hosts (up to 250). From these time-serving hosts, the system chooses one NTP host with which to synchronize. To determine which server was selected, use the <code>show ntp associations</code> command. Because many polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.														
Related Commands	show ntp associations — displays the NTP servers configured and their status.														

ntp source

Specify an interface's IP address to be included in the NTP packets.

Z9500

Syntax	<pre>ntp source interface</pre> To delete the configuration, use the <code>no ntp source</code> command.	
Parameters	interface Enter the following keywords and slot/port or number information: - For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. - For a Port Channel interface, enter the keyword <code>lag</code> then a number. The range is from 1 to 128.	

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp trusted-key

Set a key to authenticate the system to which NTP synchronizes.

Z9500

Syntax `ntp trusted-key number`
To delete the key, use the `no ntp trusted-key number` command.

Parameters

<i>number</i>	Enter a number as the trusted key ID. The range is from 1 to 4294967295.
---------------	--

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

**Usage
Information**

The `number` parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.

**Related
Commands**

[ntp authentication-key](#) — sets an authentication key for NTP.

[ntp authenticate](#) — enables the NTP authentication parameters you set.

ntp update-calendar

Configure the system to update the calendar (the hardware clock) with the NTP-derived time.

Z9500

Syntax

```
ntp update-calendar [minutes]
```

To return to default setting, use the `no ntp update-calendar` command.

Parameters

minutes (OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock. The range is from 1 to 1440. The default is **60 minutes**.

Defaults

Not enabled.

**Command
Modes**

CONFIGURATION

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

show calendar

Display the current date and time based on the switch hardware clock.

Z9500

Syntax `show calendar`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show calendar
16:33:30 UTC Tue Jun 26 2001
Dell#
```

Related Commands [show clock](#) — displays the time and date from the switch software clock.

show clock

Display the current clock settings.

Z9500

Syntax	show clock [detail]	
Parameters	detail	(OPTIONAL) Enter the keyword <code>detail</code> to view the source information of the clock.

Command Modes	- EXEC - EXEC Privilege
---------------	---

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example	Dell#show clock 11:05:56.949 UTC Thu Oct 25 2001 Dell#
---------	--

Example (Detail)	Dell#show clock detail 12:18:10.691 UTC Wed Jan 7 2009 Time source is RTC hardware Summer time starts 02:00:00 UTC Sun Mar 8 2009 Summer time ends 02:00:00 ABC Sun Nov 1 2009 Dell#
------------------	---

Related Commands	clock summer-time recurring — displays the time and date from the switch hardware clock. show calendar — displays the time and date from the switch hardware clock.
------------------	--

show ntp associations

Display the NTP master and peers.

Z9500

Syntax `show ntp associations`

- Command Modes**
- EXEC
 - EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show ntp associations` command shown in the Example below.

Field	Description
(none)	One or more of the following symbols could be displayed: • * means synchronized to this peer. • # means almost synchronized to this peer. • + means the peer was selected for possible synchronization. • - means the peer is a candidate for selection. • ~ means the peer is statically configured.
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the switch received an NTP packet.

Field	Description
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
disp	Displays the dispersion.

Example

```
Dell#show ntp associations
remote      ref clock  st when poll reach delay  offset disp
=====
 10.10.120.5 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16      377 -0.08 -1499.9
104.16
 172.31.1.33 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
 192.200.0.2 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
* master (syncd), # master (unsyncd), + selected, - candidate
Dell#
```

Related Commands

[show ntp status](#) — displays the current NTP status.

show ntp status

Display the current NTP status.

Z9500

Syntax `show ntp status`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ntp status` command shown in the Example below.

Field	Description
"Clock is..."	States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
"frequency is..."	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
"reference time is..."	Displays the reference time stamp.
"clock offset is..."	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
"root dispersion is..."	Displays the root and path dispersion.
"peer mode is..."	State what NTP mode the switch is. This should be Client mode.

Example

```
Dell#sh ntp status
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision
is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan
10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer
dispersion msec
peer mode is client
Dell#
```

Related Commands

[show ntp associations](#) — displays information on the NTP master and peer configurations.

Tunneling Commands

Tunnel interfaces create a logical tunnel for IPv4 or IPv6 traffic. You can configure DCSP, hop-limits and flow-labels. To enable a tunnel interface, use the following commands.

ip unnumbered

Configure a tunnel interface to operate without a unique IPv4 address and specify the interface from which the tunnel borrows its address.

Z9500

Syntax	ip unnumbered <i>{interface-type slot/port}</i> To set the tunnel back to default logical address use the no ip unnumbered command. If the tunnel was previously operational, the tunnel interface remains operationally down until you also configure the tunnel IPv6 address.									
Parameters	interface-type slot/port	Enter the interface type, followed by a slot and port number.								
Defaults	None									
Command Modes	INTERFACE TUNNEL									
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.4(0.1)</td><td>Introduced on the S4810, S4820T, S6000 and Z9000.</td></tr><tr><td>9.3(0.1)</td><td>Introduced on the S6000 and Z9000.</td></tr></table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.4(0.1)	Introduced on the S4810, S4820T, S6000 and Z9000.	9.3(0.1)	Introduced on the S6000 and Z9000.	
Version	Description									
9.5(0.1)	Introduced on the Z9500.									
9.4(0.1)	Introduced on the S4810, S4820T, S6000 and Z9000.									
9.3(0.1)	Introduced on the S6000 and Z9000.									
Usage Information	The <code>ip unnumbered</code> command fails in two conditions: • If the logical IP address is configured. • If the tunnel mode is IPv6IP (where an IP address over a tunnel interface is not supported). To ping an IP-unnumbered tunnel, the logical address route information must be present at both the source and destination ends of the tunnel.									



NOTE: The `ip unnumbered` command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface status is not changed to operationally up until the logical IP address is identified from the address family.

ipv6 unnumbered

Configure a tunnel interface to operate without a unique IPv6 address and specify the interface from which the tunnel borrows its address.

Z9500

Syntax

ipv6 unnumbered {interface-type slot/port}

To set the tunnel back to default logical address use the **no ipv6 unnumbered** command. If the tunnel was previously operational, the tunnel interface remains operationally down until you also configure the tunnel IPv4 address.

Parameters

interface-type slot/port

Enter the interface type, followed by a slot and port number.

Defaults

None.

Command Modes

INTERFACE TUNNEL

Command History

Version

Description

9.5(0.1)

Introduced on the Z9500.

9.4(0.0)

Introduced on the S4810, S4820T, S6000 and Z9000.

9.3(0.1)

Introduced on the S6000 and Z9000.

Usage Information

The ipv6 unnumbered command fails in two conditions:

• If the logical ip address is configured.

• If the tunnel mode is IPv6IP (where an IP address over a tunnel interface is not supported).

To ping an IPv6-unnumbered tunnels, the logical address route information must be present at both the source and destination ends of the tunnel.



NOTE:

The `ipv6 unnumbered` command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface is not changed to operationally up until the logical IP address is identified from the address family.

tunnel allow-remote

Configure the remote IPv4 or IPv6 addresses whose tunneled packets are accepted for decapsulation. If you do not configure an allow-remote address, tunneled packets from all remote peer addresses are accepted.

Z9500

Syntax	tunnel allow-remote { <i>ip-address</i> <i>ipv6-address</i> } [<i>mask</i>]	
	To delete a configured allow-remote entry, enter the no tunnel allow-remote command and specify a configured IPv4/IPv6 address and mask value. If you enter the no form of the command without an address and mask value, all configured allow-remote entries are deleted.	
Parameters	<i>ip-address</i>	Enter the source IPv4 address in A.B.C.D format.
	<i>ipv6-address</i>	Enter the source IPv6 address in X:X:X::X format.
	<i>mask</i>	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D to match a range of remote addresses. The default mask is /32 for IPv4 addresses and /128 for IPv6 addresses, which match only the specified address.
Defaults	If you do not configure a tunnel allow-remote address, all traffic destined to tunnel's source address is decapsulated.	
Command Modes	INTERFACE TUNNEL	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.
	9.3(0.1)	Introduced on the S6000 and Z9000.
Usage Information	You can configure up to eight allow-remote entries on a multipoint receive-only tunnel.	
	This command fails if the address family entered does not match the outer header address family of the tunnel mode, tunnel source, or any other tunnel allow-remote address.	
	If you configure an allow-remote address, the tunnel source or tunnel mode commands fail if the outer header address family does not match that of the configured allow-remote address.	

tunnel destination

Set a destination endpoint for the tunnel.

Z9500

Syntax	<code>tunnel destination {ip-address ipv6-address}</code> To delete a tunnel destination address, use the <code>no tunnel destination {ip-address ipv6-address}</code> command.							
Parameters	<i>ip-address</i>	Enter the destination IPv4 address for the tunnel.						
	<i>ipv6-address</i>	Enter the destination IPv6 address for the tunnel.						
Defaults	none							
Command Modes	INTERFACE TUNNEL (conf-if-tu)							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.2)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.							
Usage Information	- The tunnel interface is inoperable without a valid reachable tunnel destination address of the appropriate address type for the configured tunnel mode. - The destination address establishes a logical tunnel to the specified destination address using a destination address of the outer tunnel header. If you configure a tunnel interface or source address, the tunnel destination must be compatible for this command to function.							

tunnel dscp

Configure the method used to set the DSCP in the outer tunnel header.

Z9500

Syntax	<pre>tunnel dscp {mapped value}</pre> To use the default tunnel mapping behavior, use the <code>no tunnel dscp {mapped value}</code> command.
--------	--

Parameters	mapped	Enter the keyword mapped to map IPv6 traffic class/IPv4 DSCP to the IPv4 DCSP\IPv6 traffic class. This option copies the IPv6 traffic class/IPv4 DSCP in the encapsulated packet to the tunnel header.						
	value	Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of 0 denotes mapped traffic.						
Defaults	0 (Mapped using IPv6 traffic)							
Command Modes	INTERFACE TUNNEL (conf-if-tu)							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.2)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.							
Usage Information	- This command configures the method used to set the high 6 bits (the differentiated services codepoint) of the IPv4 TOS or the IPv6 traffic class in the outer IP header. - A value of 0 copies the original packet DSCP (IPv4) or Traffic Class (IPv6) to the tunnel header DSCP or Traffic Class. DSCP or Traffic Class depends on the tunnel mode.							

tunnel flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

Z9500

Syntax	<pre>tunnel flow-label value</pre> To return to the default value of 0, use the <code>no tunnel flow-label value</code> command.	
Parameters	value	Enter a value to set the IPv6 flow label value in the tunnel header. The range is from 0 to 1048575. The default value is 0. .

Defaults	0 (Mapped using original packet flow-label value to the tunnel header flow-label value.)						
Command Modes	INTERFACE TUNNEL (conf-if-tu)						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.2)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
Version	Description						
9.5(0.1)	Introduced on the Z9500.						
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.						
Usage Information	This command is only valid for tunnel interfaces with an IPv6 outer header.						

tunnel hop-limit

Configure the method to set the IPv4 time-to-live or the IPv6 hop limit value in the outer tunnel header.

Z9500

Syntax	<code>tunnel hop-limit value</code> To restore the default tunnel hop-limit, use the <code>no tunnel hop-limit</code> command.							
Parameters	value	Enter the hop limit (IPv6) or time-to-live (IPv4) to include in the tunnel header. The range is from 0 to 255. The default is 64.						
Defaults	64 (for IPv4 and IPv6)							
Command Modes	INTERFACE TUNNEL (conf-if-tu)							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.2)</td><td>Introduced on the Z9000, S4810, and S4820T.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
Version	Description							
9.5(0.1)	Introduced on the Z9500.							
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.							

Usage Information	A value of 0 copies the inner packet hop limit (IPv6) or time-to-live (IPv4) in the encapsulated packet to the tunnel header hop limit value.
--------------------------	---

tunnel mode

Enable a tunnel interface.

Z9500

Syntax	<code>tunnel mode {ipip ipv6 ipv6ip}</code> To disable an active tunnel interface, use the <code>no tunnel mode</code> command.
---------------	--

Parameters	ipip	Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.
	ipv6	Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.
	ipv6ip	Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.

Defaults	None.
-----------------	-------

Command Modes	INTERFACE TUNNEL (conf-if-tu)
----------------------	-------------------------------

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
------------------------	--

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.

Usage Information	This command is required to enable a tunnel interface. For the tunnel to function, you must define a tunnel mode. If the tunnel destination or source address have been previously defined, the tunnel mode must be compatible for this command to function.
--------------------------	--

tunnel source

Set a source address for the tunnel.

Z9500

Syntax

tunnel source {ip-address | ipv6-address | interface-type-number }

To delete the current tunnel source address, use the no tunnel source command.

Parameters

ip-address

Enter the source IPv4 address in A.B.C.D format.

ipv6-address

Enter the source IPv6 address in X:X:X:X::X format.

interface-type-number

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a Port Channel interface, enter the keyword port-channel then a number from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE then the slot/port information.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults

none

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

If you have configured a tunnel interface or destination address, the tunnel source must be compatible for this command to function. If you configure the tunnel source address as an interface, the tunnel does not function unless a compatible address is present on the specified interface.

If you configure the tunnel source address as tunnel source interface, the lowest address is used. This address is not changed even if you configure a lower

address on the selected interface. To change the selected address, reload or recreate the tunnel or remove the selected address from the interface.

Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with NIC teaming, automatic recovery from a failed link.

clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

Z9500

Syntax	<code>clear ufd-disable {interface <i>interface</i> uplink-state-group <i>group-id</i>}</code>	
Parameters	interface <i>interface</i>	Specify one or more downstream interfaces. For <i>interface</i>, enter one of the following interface types: • 10 Gigabit Ethernet: <code>tengigabitethernet {slot/port slot/ port-range}</code> • 40 Gigabit Ethernet: <code>fortyGigE {slot/port slot/ port-range}</code> • Port channel: <code>port-channel {1-512 port-channel-range}</code> Where <code>port-range</code> and <code>port-channel-range</code> specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: <code>tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5</code>. A comma is required to separate each port and port-range entry.
	uplink-state-group <i>group-id</i>	Re-enables all UFD-disabled downstream interfaces in the group. The valid group-id values are from 1 to 16.
Defaults	A downstream interface in a UFD-disabled uplink-state group is also disabled and is in a UFD-Disabled Error state.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

Z9500

Syntax

```
debug uplink-state-group [group-id]
```

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

Parameters

group-id	Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.
-----------------	--

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands [clear ufd-disable](#) — re-enables downstream interfaces that are in a UFD-Disabled Error state.

description

Enter a text description of an uplink-state group.

Z9500

Syntax	description text											
Parameters	text	Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.										
Defaults	none											
Command Modes	UPLINK-STATE-GROUP											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.4.2.3</td><td>Introduced on the S-Series S50.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.	8.4.2.3	Introduced on the S-Series S50.
Version	Description											
9.2(1.0)	Introduced on the Z9500.											
8.3.19.0	Introduced on the S4820T.											
8.3.12.0	Introduced on the S4810.											
8.4.2.3	Introduced on the S-Series S50.											
Example	<pre>Dell(conf-uplink-state-group-16)# description test Dell(conf-uplink-state-group-16)#</pre>											
Related Commands	uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.											

downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

Z9500

Syntax `downstream interface`

To delete an uplink-state group, enter the `no downstream interface` command.

Parameters

interface

Enter one of the following interface types:

- 10-Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
- 40-Gigabit Ethernet: `fortyGigE {slot/port | slot/port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example:
`tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Related Commands

- [upstream](#) — assigns a port or port-channel to the uplink-state group as an upstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

Z9500

Syntax

`downstream auto-recover`

To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.

Defaults

The auto-recovery of UFD-disabled downstream ports is enabled.

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

downstream disable links

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

Z9500

Syntax	<code>downstream disable links {<i>number</i> all}</code> To revert to the default setting, use the <code>no downstream disable links</code> command.	
Parameters	<i>number</i>	Enter the number of downstream links to be brought down by UFD. The range is from 1 to 1024.
	all	Brings down all downstream links in the group.
Defaults	No downstream links are disabled when an upstream link in an uplink-state group goes down.	
Command Modes	UPLINK-STATE-GROUP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information	A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down. If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.
Related Commands	downstream — assigns a port or port-channel to the uplink-state group as a downstream interface. uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

enable

Enable uplink state group tracking for a specific UFD group.

Z9500

Syntax	<code>enable</code> To disable upstream-link tracking without deleting the uplink-state group, use the <code>no enable</code> command.										
Defaults	Upstream-link tracking is automatically enabled in an uplink-state group.										
Command Modes	UPLINK-STATE-GROUP										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.4.2.3</td><td>Introduced on the S-Series S50.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T	8.3.12.0	Introduced on the S4810.	8.4.2.3	Introduced on the S-Series S50.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T										
8.3.12.0	Introduced on the S4810.										
8.4.2.3	Introduced on the S-Series S50.										
Related Commands	uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.										

show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

Z9500

Syntax	<code>show running-config uplink-state-group [group-id]</code>
Parameters	group-id Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are from 1 to 16.
Defaults	none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream TengigabitEthernet 0/2,4,6,11-19
upstream TengigabitEthernet 0/48, 52
upstream PortChannel 1
!
uplink state track 2
downstream TengigabitEthernet 0/1,3,5,7-10
upstream TengigabitEthernet 0/56,60
```

Related Commands

- [show uplink-state-group](#) — displays the status information on a specified uplink-state group or all groups.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

show uplink-state-group

Display status information on a specified uplink-state group or all groups.

Z9500

Syntax

```
show uplink-state-group [group-id] [detail]
```

Parameters

group-id	Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
detail	Displays additional status information on the upstream and downstream interfaces in each group

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

Dell#show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface
disabled
Uplink State Group      : 1 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 3 Status: Enabled, Up
Upstream Interfaces     : Te 0/46(Up) Te 0/47(Up)
Downstream Interfaces   : Te 1/0(Up) Te 1/1(Up) Te 1/3(Up) Te
1/5(Up) Te 1/6(Up)

Uplink State Group      : 5 Status: Enabled, Down
Upstream Interfaces     : Te 0/0(Dwn) Te 0/3(Dwn) Te 0/5(Dwn)
Downstream Interfaces   : Te 1/2(Dis) Te 1/4(Dis) Te 1/11(Dis)
Te 1/12(Dis) Te 1/13(Dis) Te 1/14(Dis) Te 1/15(Dis)

Uplink State Group      : 6 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 7 Status: Enabled, Up
Upstream Interfaces     :
Downstream Interfaces   :

Uplink State Group      : 16 Status: Disabled, Up
Upstream Interfaces     : Te 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces   : Te 0/40(Dwn)
```

Related
Commands

- [show running-config uplink-state-group](#) — displays the current configuration of one or more uplink-state groups.
- [uplink-state-group](#) — create an uplink-state group and enables the tracking of upstream links.

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

Z9500

Syntax

`uplink-state-group group-id`
To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

Parameters

group-id Enter the ID number of an uplink-state group. The range is from 1 to 16.

Defaults

none

Command
Modes

CONFIGURATION

Command
History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage
Information

After you enter the command, to assign upstream and downstream interfaces to the group, enter Uplink-State-Group Configuration mode.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in uplink-state-group configuration mode.

Example

```
Dell(conf)#uplink-state-group 16
Dell(conf-uplink-state-group-16)#Dec 3 00:46:45: %SYSTEM:CP
%IFMGR-5-ASTATE_UP: Changed uplink state group
Admin state to up: Group 16
```

Related Commands

- [show running-config uplink-state-group](#) — displays the current configuration of one or more uplink-state groups.
- [show uplink-state-group](#) — displays the status information on a specified uplink-state group or all groups.

upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

Z9500

Syntax

`upstream interface`

To delete an uplink-state group, use the `no upstream interface` command.

Parameters

interface

Enter one of the following interface types:

- 10-Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
- 40-Gigabit Ethernet: `fortyGigE {slot/port | slot/port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Example

```
Dell(conf-uplink-state-group-16) # upstream tengigabitethernet
1/10-15
Dell(conf-uplink-state-group-16) #
```

Related Commands

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can “stack” VLANs into one tunnel and switch them through the network transparently.

For more information about basic VLAN commands, refer to the *Virtual LAN (VLAN) Commands* section in the [Layer 2](#) chapter.

Important Points to Remember

- If you do not enable the spanning tree protocol (STP) across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer’s networks are tunneled across the stackable VLAN network.
- If you do enable STP across the stackable VLAN network, STP BPDUs from the customer’s networks are consumed and not tunneled across the stackable VLAN network unless you enable protocol tunneling.



NOTE: For more information about protocol tunneling on the E-Series, refer to [Service Provider Bridging](#).

- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN are not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) management over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- Dell Networking recommends that you do not use the same MAC address, on different customer VLANs, on the same stackable VLAN.
- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands do not switch traffic for the default VLAN. These interfaces are switch traffic only when they are added to a non-default VLAN.
- Starting with the Dell Networking OS version 7.8.1 for C-Series and S-Series (Dell Networking OS version 7.7.1 for E-Series, 8.2.1.0 for E-Series ExaScale), a vlan-stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the vlan-stack trunk port is also a member of an untagged vlan, the port must be in Hybrid mode. Refer to [portmode hybrid](#).

member

Assign a stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

Z9500

Syntax `member interface`

To remove an interface from a Stackable VLAN, use the `no member interface` command.

Parameters

interface	Enter the following keywords and slot/port or number information:
	• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/ port information.

Defaults Not configured.

Command Modes CONF-IF-VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information You must enable the stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.

Related Commands [vlan-stack compatible](#) — enables stackable VLAN on a VLAN.

vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

Z9500

Syntax	<code>vlan-stack access</code> To remove access port designation, use the <code>no vlan-stack access</code> command.														
Defaults	Not configured.														
Command Modes	INTERFACE														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></tbody></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the C-Series and S-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
8.2.1.0	Introduced on the E-Series ExaScale.														
7.6.1.0	Introduced on the C-Series and S-Series.														
Usage Information	Prior to enabling this command, to place the interface in Layer 2 mode, enter the <code>switchport</code> command. To remove the access port designation, remove the port (using the <code>no member interface</code> command) from all stackable VLAN enabled VLANs.														

vlan-stack compatible

Enable the stackable VLAN feature on a VLAN.

Z9500

Syntax	<code>vlan-stack compatible</code> To disable the Stackable VLAN feature on a VLAN, use the <code>no vlan-stack compatible</code> command.
---------------	---

Defaults

Command Modes

Command History

Not configured.

CONF-IF-VLAN

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information

Prior to disabling the stackable VLAN feature, remove the members.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

Example

```
Dell#show vlan
```

Codes: * - Default VLAN, G - GVRP VLANs

NUM	Status	Q	Ports
* 1	Inactive		
2	Active	M	Te 2/13
		M	Te 2/0-2
3	Active	M	Pol(Te 2/14-15)
		M	Te 2/18
		M	Te 2/3
4	Active	M	Pol(Te 2/14-15)
		M	Te 2/18
		M	Te 2/4
5	Active	M	Pol(Te 2/14-15)
		M	Te 2/18
		M	Te 2/5

```
Dell#
```

vlan-stack dot1p-mapping

Map C-Tag dot1p values to a S-Tag dot1p value. You can separate the C-Tag values by commas and dashed ranges are permitted. Dynamic mode CoS overrides any Layer 2 QoS configuration in case of conflicts.

Z9500

Syntax `vlan-stack dot1p-mapping c-tag-dot1p values sp-tag-dot1p value`

Parameters	c-tag-dot1p value	Enter the keyword <code>c-tag-dot1p</code> then the customer dot1p value that is mapped to a service provider dot1p value. The range is from 0 to 7.
	sp-tag-dot1p value	Enter the keyword <code>sp-tag-dot1p</code> then the service provider dot1p value. The range is from 0 to 7.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the C-Series and S-Series.

vlan-stack protocol-type

Define the stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, the system assigns the value 0x9100.

Z9500

Syntax `vlan-stack protocol-type number`

Parameters	number	Enter the hexadecimal number as the stackable VLAN tag. You may specify both bytes of the 2-byte S-Tag TPID. The range is from 0 to FFFF. The default is 9100 .
-------------------	---------------	--

Defaults	0x9100														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.	8.2.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the C-Series and S-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.7.0	Introduced on the S4810.														
8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.														
8.2.1.0	Introduced on the E-Series ExaScale.														
7.6.1.0	Introduced on the C-Series and S-Series.														
Usage Information	For specific interoperability limitations regarding the S-Tag TPID, refer to the <i>Dell Networking OS Configuration Guide</i>. The four characters you enter in the CLI for number are interpreted, as shown in the following table. <table> <tr> <th>Number</th><th>Resulting TPID</th></tr> <tr> <td>1</td><td>0x0001</td></tr> <tr> <td>10</td><td>0x0010</td></tr> <tr> <td>81</td><td>0x0081</td></tr> <tr> <td>8100</td><td>0x8100</td></tr> </table>	Number	Resulting TPID	1	0x0001	10	0x0010	81	0x0081	8100	0x8100				
Number	Resulting TPID														
1	0x0001														
10	0x0010														
81	0x0081														
8100	0x8100														
Related Commands	portmode hybrid — sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays. vlan-stack trunk — specifies a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.														

vlan-stack trunk

Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

Z9500

Syntax	<code>vlan-stack trunk</code> To remove a trunk port designation from the selected interface, use the <code>no vlan-stack trunk</code> command.																		
Defaults	Not configured.																		
Command Modes	INTERFACE																		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Netowrking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.</td></tr><tr><td>7.8.1.0</td><td>Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port.</td></tr><tr><td>7.7.1.0</td><td>Functionality augmented for E-Series to enable multi-purpose use of the port.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.	7.8.1.0	Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port.	7.7.1.0	Functionality augmented for E-Series to enable multi-purpose use of the port.	7.6.1.0	Introduced on the C-Series and S-Series.
Version	Description																		
9.2(1.0)	Introduced on the Z9500.																		
8.3.19.0	Introduced on the S4820T.																		
8.3.11.1	Introduced on the Z9000.																		
8.3.7.0	Introduced on the S4810.																		
8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.																		
7.8.1.0	Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port.																		
7.7.1.0	Functionality augmented for E-Series to enable multi-purpose use of the port.																		
7.6.1.0	Introduced on the C-Series and S-Series.																		

In Example 2, the tag protocol identifier (TPID) is set to 88A8. The “Te 2/10” port is configured to act as a VLAN-Stack access port, while the “Te 1/0” port acts as a VLAN-Stack trunk port, switching stackable VLAN traffic for VLAN 10, while also switching untagged traffic for VLAN 30 and tagged traffic for VLAN 40. (To allow VLAN 30 traffic, the native VLAN feature is required, by executing the `portmode hybrid` command. Refer to [portmode hybrid](#) in Interfaces.

Example 1

```
Dell(conf-if-te-0/42)#switchport
Dell(conf-if-te-0/42)#vlan-stack trunk
Dell(conf-if-te-0/42)#show config
!
interface TenGigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
Dell(conf-if-te-0/42)#interface vlan 100
Dell(conf-if-vl-100)#vlan-stack compatible
Dell(conf-if-vl-100-stack)#member gigabitethernet 0/42
Dell(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member TenGigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-100-stack)#interface vlan 20
Dell(conf-if-vl-20)#tagged tengigabitethernet 0/42
Dell(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged TenGigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-20)#do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

   NUM  Status Description      Q Ports
* 1      Inactive
   20    Active                  T Te 0/42
  100    Active                  M Te 0/42
Dell(conf-if-vl-20)#
```

Example 2

```
Dell(config)#vlan-stack protocol-type 88A8
Dell(config)#interface tengigabitethernet 2/10
Dell(conf-if-te-2/10)#no shutdown
Dell(conf-if-te-2/10)#switchport
Dell(conf-if-te-2/10)#vlan-stack access
Dell(conf-if-te-2/10)#exit

Dell(config)#interface tenGigabitethernet 1/0
Dell(conf-if-te-1/0)#no shutdown
Dell(conf-if-te-1/0)#portmode hybrid
Dell(conf-if-te-1/0)#switchport
Dell(conf-if-te-1/0)#vlan-stack trunk
Dell(conf-if-te-1/0)#exit
```

```
Dell(config)#interface vlan 10
Dell(conf-if-vlan)#vlan-stack compatible
Dell(conf-if-vlan)#member Te 0/0, Te 1/0, Te 2/10
Dell(conf-if-vlan)#exit

Dell(config)#interface vlan 30
Dell(conf-if-vlan)#untagged TenGi 1/0
Dell(conf-if-vlan)#exit
Dell(config)#

Dell(config)#interface vlan 40
Dell(conf-if-vlan)#tagged TenGi 1/0
Dell(conf-if-vlan)#exit
Dell(config)#
```

Virtual Link Trunking (VLT)

Virtual link trunking (VLT) allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology.

VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

 **NOTE:** When you launch the VLT link, the VLT peer-ship is not established if any of the following is **TRUE**:

- The VLT System-MAC configured on both the VLT peers do not match.
- The VLT Unit-Id configured on both the VLT peers are identical.
- The VLT System-MAC or Unit-Id is configured only on one of the VLT peers.
- The VLT domain ID is not the same on both peers.

If the VLT peer-ship is already established, changing the System-MAC or Unit-Id does not cause VLT peer-ship to go down.

Also, if the VLT peer-ship is already established and the VLT Unit-Id or System-MAC are configured on both peers, then changing the CLI configurations on the VLT Unit-Id or System-MAC is rejected if any of the following become **TRUE**:

- After making the CLI configuration change, the VLT Unit-Id becomes identical on both peers.
- After making the CLI configuration change, the VLT System-MAC do not match on both peers.

When the VLT peer-ship is already established, you can remove the VLT Unit-Id or System-MAC configuration from either or both peers. However, removing configuration settings can cause the VLT ports to go down if you configure the Unit-Id or System-MAC on only one of the VLT peers.

back-up destination

Configure the IPv4 or IPv6 address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

Z9500

Syntax `back-up destination {[ipv4-address] | [ipv6 ipv6-address]
[interval seconds]}`

Parameters `ipv4-address` Enter the IPv4 address of the backup destination.

clear vlt statistics

Clear the statistics on VLT operations.

Z9500

Syntax	<code>clear vlt statistics [arp domain igmp-snoop mac multicast ndp]</code>	
Parameters	domain	Clear the VLT statistics for the domain.
	multicast	Clear the VLT statistics for multicast.
	mac	Clear the VLT statistics for the MAC address.
	arp	Clear the VLT statistics for ARP.
	igmp-snoop	Clear the VLT statistics for IGMP snooping.

	ndp	Clear the VLT statistics for NDP.																
Command Modes	EXEC																	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.2(0.2)</td><td>Added <code>multicast</code> and <code>ndp</code> parameters.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.2(0.2)	Added <code>multicast</code> and <code>ndp</code> parameters.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description																	
9.5(0.1)	Introduced on the Z9500.																	
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.																	
9.2(0.2)	Added <code>multicast</code> and <code>ndp</code> parameters.																	
9.0.2.0	Introduced on the S6000.																	
9.0.0.0	Introduced on the Z9000.																	
8.3.19.0	Introduced on the S4820T.																	
8.3.12.0	Introduced on the S4810.																	
Example	<pre>VLT ARP Statistics ----- ARP Tunnel Pkts sent:0 ARP Tunnel Pkts Rcvd:0 ARP-sync Pkts Sent:0 ARP-sync Pkts Rcvd:0 ARP Reg Request sent:19 ARP Reg Request rcvd:10</pre>																	
Related Commands	show vlt statistics — displays statistics on VLT operations.																	

delay-restore

Configure the delay in bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.

Z9500

Syntax	<code>delay-restore</code>	
Parameters	delay-restore	Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLTi device is reloaded or after the peer-link is restored between VLT peer switches. The range from 1 to 1200. The default is 90 seconds .

Defaults	Not configured.														
Command Modes	VLT DOMAIN														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S8420T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S8420T.	8.3.12.0	Introduced on the S4810.
Version	Description														
9.5(0.1)	Introduced on the Z9500.														
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.														
9.0.2.0	Introduced on the S6000.														
9.0.0.0	Introduced on the Z9000.														
8.3.19.0	Introduced on the S8420T.														
8.3.12.0	Introduced on the S4810.														
Usage Information	To delay the system from bringing up the VLT port for a brief period to allow IGMP Snooping and Layer 3 routing protocols to converge, use the <code>delay-restore</code> parameter. Use this feature: • after a VLT device is reloaded. • if the Peer VLT device was up at the time the VLTi link failed to the time when it was restored.														
Related Commands	show vlt statistics — displays statistics on VLT operations.														

lacp ungroup member-independent

Prevent possible loop during the bootup of a VLT peer switch or a device that accesses the VLT domain.

Z9500

Syntax	<code>lacp ungroup member-independent {vlt port-channel}</code>	
Parameters	port-channel	Force all LACP port-channel members to become switchports.
	vlt	Force all VLT LACP members to become switchports.
Defaults	Not configured.	

Command Modes	CONFIGURATION																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Added port-channel parameter on the S4810.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Added port-channel parameter on the S4810.	8.3.8.0	Introduced on the S4810.
Version	Description																
9.5(0.1)	Introduced on the Z9500.																
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.																
9.0.2.0	Introduced on the S6000.																
9.0.0.0	Introduced on the Z9000.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Added port-channel parameter on the S4810.																
8.3.8.0	Introduced on the S4810.																
Usage Information	LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device. On the S4810, during boot-up in a stacking configuration, the system must be able to reach the DHCP server with the boot image and configuration image. During boot-up, only untagged DHCP requests are sent to the DHCP server to receive an offer on static LAGs between switches. The DHCP server must be configured to start in BMP mode. If switches are connected using LACP port-channels like the VLT peer and Top of Rack (ToR), use the port-channel parameter on the ToR-side configuration to allow member ports of an ungrouped LACP port-channel to inherit vlan membership of that port channel to ensure untagged packets that are sent by a VLT peer device reach the DHCP server located on the ToR. To ungroup the VLT and port-channel configurations, use the no lacp ungroup member independent command on a VLT port channel, depending on whether the port channel is VLT or non-VLT.																
Example	<pre> Dell(conf)#lacp ungroup member-independent ? port-channel LACP port-channel members become switchports vlt All VLT LACP members become switchports </pre>																

multicast peer-routing timeout

Configure the time for a VLT node to retain synced multicast routes or synced multicast outgoing interface (OIF) after a VLT peer node failure.

Z9500

Syntax `multicast peer-routing timeout value`
To restore the default value, use the `no multicast peer-routing timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.
--------------	--

Command Modes VLT DOMAIN (conf-vlt-domain)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

Z9500

Syntax `peer-link port-channel port-channel-number {peer-down-vlan vlan id}`

Parameters

port-channel-number	Enter the port-channel number that acts as the interconnect trunk.
peer-down-vlan vlan id	Enter the keyword <code>peer-down-vlan</code> then a VLAN ID to configure the VLAN that the VLT peer link uses when the VLT peer is down.

Defaults	Not configured.																
Command Modes	VLT DOMAIN																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Added support for the peer-down-vlan parameter.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced on the S4810.</td></tr> </tbody> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Added support for the peer-down-vlan parameter.	8.3.8.0	Introduced on the S4810.
Version	Description																
9.5(0.1)	Introduced on the Z9500.																
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.																
9.0.2.0	Introduced on the S6000.																
9.0.0.0	Introduced on the Z9000.																
8.3.19.0	Introduced on the S4820T.																
8.3.12.0	Added support for the peer-down-vlan parameter.																
8.3.8.0	Introduced on the S4810.																
Usage Information	To configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down, use the peer-down-vlan parameter. When a VLT peer with bare metal provisioning (BMP) is booting up, it sends untagged DHCP discover packets to its peer over the VLTi. To ensure that the DHCP discover packets are forwarded to the VLAN that has the DHCP server, use this configuration.																

peer-routing

Enable L3 VLT peer-routing. This command is applicable for both IPV6/ IPV4.

Z9500

Syntax	<pre>peer-routing</pre> To disable L3 VLT peer-routing, use the <code>no peer-routing</code> command.
Defaults	Disabled.
Command Modes	VLT DOMAIN (conf-vlt-domain)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the support for IPV6 / IPV4.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	ntroduced on the Z9000, S4810, and S4820T.

peer-routing-timeout

Configure the delay after which peer routing is disabled when the peer is unavailable. This command is applicable for both IPV6/ IPV4.

Z9500

Syntax `peer-routing-timeout value`
To restore the default value, use the `no peer-routing-timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).
--------------	--

Command Modes VLT DOMAIN (conf-vlt-domain)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the support for IPV6 / IPV4.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

Usage Information When the timer expires, the software checks to see if the VLT peer is now available. If the VLT peer is not available, peer-routing is disabled on that peer.

primary-priority

Assign the priority for master election among VLT peers.

Z9500

Syntax	[no] primary-priority													
Parameters	value	To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535.												
Default	32768													
Command Modes	VLT DOMAIN													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced on the S4810.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.													
9.0.2.0	Introduced on the S6000.													
8.3.19.0	Introduced on the S4820T.													
8.3.8.0	Introduced on the S4810.													
Usage Information	After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the Dell Networking OS software elects a primary and secondary VLT peer device. To reconfigure the primary role of VLT peer switches, use the <code>priority</code> command.													

show vlt brief

Displays summarized status information about VLT domains currently configured on the switch.

Z9500

Syntax	<code>show vlt brief</code>
Default	Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information The version shown in the `show vlt brief` output command displays the VLT version number which is different from the Dell Networking OS version number. VLT version numbers are begin with odd numbers such as 3 or 5.

Example (Brief)

```
Dell(conf) #show vlt brief
VLT Domain Brief
-----

Domain ID:                        10
Role:                             Primary
Role Priority:                     32768
ICL Link Status:                  Up
Heart Beat Status:                Not Established
VLT Peer Status:                 Up
Version:                          5 (1)
Local System MAC address:         00:01:e8:8b:14:3c
Remote System MAC address:        00:01:e8:8b:15:20
Remote Sytem Version:             5 (1)
Delay-Restore timer:              90 seconds
```

show vlt backup-link

Displays information on the backup link operation.

Z9500

Syntax `show vlt backup-link`

Default Not configured.

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell_VLTpeer1# show vlt backup-link

VLT Backup Link
-----
Destination:                10.11.200.18
Peer HeartBeat status:      Up
HeartBeat Timer Interval:   1
HeartBeat Timeout:          3
UDP Port:                   34998
HeartBeat Messages Sent:    1026
HeartBeat Messages Received: 1025
```

show vlt counters

Displays the counter information.

Z9500

Syntax

```
show vlt counters [arp| igmp-snoop | interface | mac | ndp]
```

Parameters

arp	Enter the keyword <code>arp</code> to display the ARP counter information for the VLT.
igmp-snoop	Enter the keywords <code>igmp-snoop</code> to display the igmp-snooping counter information for the VLT.
interface	Enter the keyword <code>interface</code> to display the interface counter information for the VLT.
mac	Enter the keyword <code>mac</code> to display the MAC address counter information for the VLT.
ndp	Enter the keyword <code>ndp</code> to display the VLT counter information for NDP.

Default	Not configured.												
Command Modes	EXEC												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.0.2.0	Introduced on the S6000.												
9.0.0.0	Introduced on the Z9000.												
8.3.19.0	Introduced on the S4820T.												
8.3.12.0	Introduced on the S4810.												
Usage Information	If you do not add a parameter such as <code>arp</code> or <code>mac</code> , the output displays all of the counters.												
Example	<pre> Dell# show vlt counter Total VLT counters ----- L2 Total MAC-Address Count : IGMP MRouter Vlans count : IGMP Mcast Groups count : ARP entries count : </pre>												
Example (igmp-snoop)	<pre> Dell# show vlt counter igmp-snoop Total IGMP VLT counters ----- IGMP MRouter Vlans count : 1 IGMP Mcast Groups count : 5 </pre>												
Example (igmp-snoop interface port-channel)	<pre> Dell#show vlt counter igmp-snoop interface port-channel 2 VLT Port-ID: 2 IGMP Counter ----- IGMP MRouter Vlans count : 0 IGMP Mcast Groups count : 5 Dell# show vlt counter igmp-snoop interface port-channel 100 VLT Port-ID: 100 IGMP Counter ----- IGMP MRouter Vlans count : 1 IGMP Mcast Groups count : 0 Ve </pre>												
Example (NDP and Non-VLT ARP)	<pre> Dell#show vlt counters Total VLT Counters ----- L2 Total MAC-Address Count: 2 Total Arp Entries Learnt : 0 Total Arp Entries Synced : 0 Total Non-VLT Arp entries Learnt: 0 </pre>												

```

Total Non-VLT Arp Entries Synced          0
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
Total VLT Ndp Entries Learnt :            2
Total VLT Ndp Entries Synced :            0
Total Non-VLT Ndp Entries Learnt :        0
Total Non-VLT Ndp Entries Synced :        0

```

show vlt detail

Displays detailed status information about VLT domains currently configured on the switch.

Z9500

Syntax `show vlt detail`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```

Dell# Dell(conf-if-vl-100)#show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
-----
10          10      UP          UP          100, 200, 300,
400,

```

show vlt inconsistency

Display run-time inconsistencies in the incoming interface (IIF) for spanned multicast routes.

Z9500

Syntax `show vlt inconsistency ip mroute`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

Example Dell#show vlt inconsistency ip mroute
Spanned Multicast Routing IIF Inconsistency

Multicast Route	LocalIIF	PeerIIF
-----	-----	-----
(22.22.22.200, 225.1.1.2)	VLAN 5	VLAN 6
(*, 225.1.1.2)	VLAN 15	te 0/5

Dell#

show vlt mismatch

Display mismatches in VLT parameters.

Z9500

Syntax `show vlt mismatch`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.

Example

```

Dell#show vlt mismatch
Domain
-----
Parameters          Local          Peer
-----
Unit-ID             0              15

Vlan-config
-----
Vlan-ID             Local Mode      Peer Mode
-----
100                  --              L3

Vlan IPv4 Multicast Status
-----
Vlan-ID             Local Status      Peer Status
-----
4094                 Active             Inactive

Dell#

```

show vlt private-vlan

Display the private VLAN (PVLAN) associated with the VLT LAG for VLT peer nodes.

Syntax `show vlt private-vlan`

Command Modes EXEC

Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S6000.
	9.3(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information If you add an ICL or VLTi link as a member of a primary VLAN, the ICL becomes a part of the primary VLAN and its associated secondary VLANs, similar to the behavior for normal trunk ports. VLAN symmetry is not validated if you associate an ICL to a PVLAN. Similarly, if you dissociate an ICL from a PVLAN, although the PVLAN symmetry exists, ICL is removed from that PVLAN in such a case. The **ICL**

Status field denotes the type of the VLAN port of the VLTi link configured in a PVLAN.

Example

```
Dell#show vlt private-vlan vlan-id

Codes: C- Community, I - Isolated, V - Internally tagged, T -
tagged, * - VLT Pvlan
Primary      Secondary      ICL Status
10
              20 (C)         V
              30 (I)         V

40
              50 (C)         T
              60 (I)         T
```

show vlt role

Displays the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the local VLT device.

Z9500

Syntax `show vlt role`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell_VLTpeer1# show vlt role

VLT Role
-----
VLT Role: Primary
System MAC address: 00:01:e8:8a:df:bc
System Role Priority: 32768
Local System MAC address: 00:01:e8:8a:df:bc
Local System Role Priority: 32768
```

```

Dell_VLTpeer2# show vlt role

VLT Role
-----
VLT Role:                Secondary
System MAC address:      00:01:e8:8a:df:bc
System Role Priority:     32768
Local System MAC address: 00:01:e8:8a:df:e6
Local System Role Priority: 32768

```

show vlt statistics

Displays statistics on VLT operations.

Z9500

Syntax	<code>show vlt statistics [arp domain igmp-snoop mac multicast ndp]</code>												
Parameters	domain Display the VLT statistics for the domain. multicast Display the VLT statistics for multicast. mac Display the VLT statistics for the MAC address. arp Display the VLT statistics for ARP. igmp-snoop Display the VLT statistics for IGMP snooping. ndp Display the VLT statistics for NDP.												
Default	Not configured.												
Command Modes	EXEC												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.2)</td><td>Added parameters <code>multicast</code> and <code>ndp</code></td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.2)	Added parameters <code>multicast</code> and <code>ndp</code>	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.
Version	Description												
9.5(0.1)	Introduced on the Z9500.												
9.2(0.2)	Added parameters <code>multicast</code> and <code>ndp</code>												
9.0.2.0	Introduced on the S6000.												
9.0.0.0	Introduced on the Z9000.												
8.3.19.0	Introduced on the S4820T.												

Version	Description
8.3.12.0	Added support in the output for ARP, MAC, and IGMP snooping.
8.3.8.0	Introduced on the S4810.

Related Commands

[clear vlt statistics](#) — clears the statistics on VLT operations.

Example



NOTE: The following example shows the statistics for *all* of the VLT parameters. If you enter a specific keyword, such as `mac`, only the statistics for that VLT parameter displays.

```
Dell VLTpeer1#show vlt statistics
VLT Statistics
-----
HeartBeat Messages Sent:      930
HeartBeat Messages Received: 909
ICL Hello's Sent:             927
ICL Hello's Received:         910
Domain Mismatch Errors:       0
Version Mismatch Errors:      0
Config Mismatch Errors:       0

VLT MAC Statistics
-----
L2 Info Pkts sent:6, L2 Mac-sync Pkts Sent:0
L2 Info Pkts Rcvd:3, L2 Mac-sync Pkts Rcvd:2
L2 Reg Request sent:1
L2 Reg Request rcvd:2
L2 Reg Response sent:1
L2 Reg Response rcvd:1

VLT Igmp-Snooping Statistics
-----
IGMP Info Pkts sent:      4
IGMP Info Pkts Rcvd:      1
IGMP Reg Request sent:    1
IGMP Reg Request rcvd:    2
IGMP Reg Response sent:   1
IGMP Reg Response rcvd:   1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcvd: 10
IGMP Tunnel PDUs sent:    10
IGMP Tunnel PDUs rcvd:    19

VLT Multicast Statistics
-----
Info Pkts Sent:           4
Info Pkts Rcvd:           2
Reg Request Sent:         2
Reg Request Rcvd:         2
Reg Response Sent:        1
Reg Response Rcvd:        0
Route updates sent to Peer: 0
Route updates rcvd from Peer: 0
Route update pkts sent to Peer: 0
Route update pkts rcvd from Peer: 0

VLT NDP Statistics
-----
```

```

NDP NA VLT Tunnel Pkts sent:16
NDP NA VLT Tunnel Pkts Rcvd:46
NDP NA Non-VLT Tunnel Pkts sent:0
NDP NA Non-VLT Tunnel Pkts Rcvd:0
Ndp-sync Pkts Sent:144
Ndp-sync Pkts Rcvd:105
Ndp Reg Request sent:25
Ndp Reg Request rcvd:24

```

show vlt statistics igmp-snoop

Displays the informational packets and IGMP control PDUs that are exchanged between VLT peer nodes.

Z9500

Syntax `show vlt statistics igmp-snoop`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```

Dell VLTpeer1#show vlt statistics igmp-snoop
VLT Igmp-Snooping Statistics
-----
IGMP Info Pkts sent:      4
IGMP Info Pkts Rcvd:     1
IGMP Reg Request sent:   1
IGMP Reg Request rcvd:   2
IGMP Reg Response sent:  1
IGMP Reg Response rcvd:  1
IGMP PDU Tunnel Pkt sent:5
IGMP PDU Tunnel Pkt rcvd:10
IGMP Tunnel PDUs sent:   10
IGMP Tunnel PDUs rcvd:   19

```

system-mac

Reconfigure the default MAC address for the domain.

Z9500

Syntax	system-mac mac-address													
Parameters	mac-address	Enter the system MAC address for the VLT domain.												
Defaults	Not configured.													
Command Modes	VLT DOMAIN													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced on the S4810.
Version	Description													
9.5(0.1)	Introduced on the Z9500.													
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.													
9.0.0.0	Introduced on the Z9000.													
8.3.19.0	Introduced on the S4820T.													
8.3.8.0	Introduced on the S4810.													
Usage Information	When you create a VLT domain on a switch, Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations. To reconfigure the default MAC address for the domain by entering a new MAC address in the format nn:nn:nn:nn:nn:nn, use the <code>system-mac</code> command. You must also reconfigure the same MAC address on the VLT peer switch.													

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

Z9500

Syntax	<code>unit-id [0 1]</code>
--------	------------------------------

Parameters	0 1	Configure the default unit ID of a VLT peer switch. Enter 0 for the first peer or enter 1 for the second peer.														
Defaults	Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.															
Command Modes	VLT DOMAIN															
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced on the S4810.
Version	Description															
9.5(0.1)	Introduced on the Z9500.															
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.															
9.0.2.0	Introduced on the S6000.															
9.0.0.0	Introduced on the Z9000.															
8.3.19.0	Introduced on the S4820T.															
8.3.8.0	Introduced on the S4810.															
Usage Information	When you create a VLT domain on a switch, Dell Networking OS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the <code>unit-id</code> command to explicitly configure the unit ID of a VLT peer. Configure a different unit ID (0 or 1) on each peer switch. To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.															

vlt domain

Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

Z9500

Syntax	<code>vlt domain domain-id</code>	
Parameters	<i>domain-id</i>	Enter the Domain ID number. Configure the same domain ID on the peer switch. The range of domain IDs is from 1 to 1000.

Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.8.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.5(0.1)	Introduced on the Z9500.	9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.	8.3.19.0	Introduced on the S4820T.	8.3.8.0	Introduced on the S4810.
Version	Description														
9.5(0.1)	Introduced on the Z9500.														
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.														
9.0.2.0	Introduced on the S6000.														
9.0.0.0	Introduced on the Z9000.														
8.3.19.0	Introduced on the S4820T.														
8.3.8.0	Introduced on the S4810.														
Usage Information	The VLT domain ID must be the same between the two VLT devices. If the domain ID is not the same, a syslog message is generated and VLT does not launch.														
Related Commands	show vlt — uses the <code>show vlt brief</code> command to display the delay-restore value.														

vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

Z9500

Syntax	<code>vlt-peer-lag port-channel <i>id-number</i></code>
Parameters	<i>id-number</i> Enter the respective vlt port-channel number of the peer device.
Defaults	Not configured.
Command Modes	INTERFACE PORT-CHANNEL
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

VLT Proxy Gateway

You can configure a proxy gateway in VLT domains. A proxy gateway enables you to locally route the packets that are destined to a L3 endpoint in another VLT domain.

proxy-gateway lldp

Configure the LLDP proxy gateway

Z9500

Syntax	proxy-gateway lldp	
Command Modes	VLT DOMAIN	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	The configuration is cached and sent to LLDP only in one of the following conditions:	
	1) The port-channel connecting the two VLT domains, across DC, must be a VLT LAG	
	2) The protocol lldp command is globally enabled	
	3) The proxy-gateway LLDP configuration is applied.	
	However, "proxy-gateway lldp" configuration is sent to the Layer 2 application. When LLDP sends an IPC reply message, SWPQ is created towards LLDP to send further updates to LLDP. When the proxy gateway peer-domain-link port-channel command is provisioned, the configuration is sent to LLDP if the port-channel is a VLT port-channel. However it will not check whether the port-channel is up or down. LLDP determines the addition and removal of LAG ports and transmits LLDP packets out accordingly.	
Example	Dell(conf)#vlt-domain 1 Dell(conf-vlt-domain)#proxy-gateway lldp	

proxy-gateway static

Configure the VLT static proxy gateway

Z9500

Syntax	[no] proxy-gateway static	
Command Modes	VLT DOMAIN	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	When proxy-gateway static configuration is made, the setting is saved in the Layer 2 application. When you remove the static proxy gateway configuration, each proxy-gateway static mac configured is deleted and also the notification to delete the local destination address (DA) configured is sent to the Layer 2 module. When remote-mac-address <i>mac-address-identifier</i> configuration is made, the MAC details are saved. When no remote-mac-address <i>mac-address-identifier</i> configuration is made, the MAC details and the local DA information are deleted.	
Example	Dell(conf)#vlt-domain 1 Dell(conf-vlt-domain)#proxy-gateway static	

remote-mac-address exclude-vlan

Configure the proxy-gateway static entry and exclude a VLAN or a range of VLANs from proxy routing.

Z9500

Syntax	remote-mac-address <i>mac-address</i> exclude-vlan <i>vlan-range</i>	
Parameters	remote-mac-address	Specify the remote MAC address for a static proxy gateway.
	mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
	vlan-range	Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10

Combination: 3, 4, 5-10, 8

Command Modes	VLT DOMAIN PROXY GW STATIC	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	You can configure the remote MAC address of the VLT peer to be associated with the static VLT proxy gateway and exclude a VLAN or a range of VLANs from proxy routing. This parameter is for a static VLT proxy gateway configuration.	
Example	<pre>Dell(conf)#vlt-domain 1 Dell(conf-vlt-domain)#proxy-gateway static Dell(conf-vlt-domain-proxy-gw-static)#remote-mac-address 00:01:e8:06:95:ac exclude-vlan 3</pre>	

peer-domain-link port-channel exclude-vlan

Configure proxy-gateway LLDP, specify a port-channel and a VLAN or range of VLANs, and exclude a VLAN or a range of VLANs from proxy routing.

Z9500

Syntax	<pre>[no] peer-domain-link port-channel <i>interface-identifier</i> exclude-vlan <i>vlan-range</i></pre>	
Parameters	port-channel	Configure the proxy-gateway interface port-channel. Port channel range is from 1 to 128.
	vlan-range	Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example:
		Comma-separated: 3, 4, 6
		Range: 5-10
		Combination: 3, 4, 5-10, 8

Command Modes	VLT DOMAIN PROXY GW LLDP
----------------------	--------------------------

Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	You can configure the port channel interface that must be associated with the LLDP proxy gateway and exclude a VLAN or a range of VLANs from proxy routing. This parameter is for an LLDP proxy gateway configuration.	
Example	<pre>Dell(conf)#vlt-domain 1 Dell(conf-vlt-domain)#proxy-gateway lldp Dell(conf-vlt-domain-proxy-gw-lldp)#peer-domain-link port-channel 20 exclude-vlan 3</pre>	

proxy-gateway peer-timeout

Configure the proxy-gateway VLT peer timeout value.

Z9500

Syntax	<code>[no] peer-timeout value</code>	
Parameters	value	Enter the timeout value in seconds. The range is from 1 to 65535. The default is infinity.
Command Modes	VLT DOMAIN PROXY GW LLDP	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	In a square VLT topology with only one link connecting remote peers, a node must stop sending its VLT peer MAC address ("vlt-peer-mac transmit" enabled) when the VLT peer is down. If you configure this time out interval, it will keep sending its peer's MAC address until the timer expires.	
Example	<pre>Dell(conf-vlt-domain-proxy-gw-lldp)# peer-timeout 5</pre>	

vlt-peer-mac transmit

Configures a peer to send its VLT peer's MAC address along with its LLDP TLV.

Z9500

Syntax	[no] vlt-peer-mac transmit	
Command Modes	VLT DOMAIN PROXY GW LLDP	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.
Usage Information	In a square VLT topology with only one link connecting remote peers, if you configure this command, any node has to send its VLT peer's MAC address along with its own MAC address to the remote VLT domain. By default, a node will send only its own MAC address to the remote VLT domain. This parameter is applicable for an LLDP proxy gateway configuration.	
Example	Dell (conf-vlt-domain-proxy-gw-lldp) # vlt-peer-mac transmit	

show vlt-proxy-gateway

Display the VLT proxy gateway configuration.

Z9500

Syntax	show vlt-proxy-gateway info {lldp static}	
Parameters	lldp	Display details about the LLDP VLT proxy gateway configuration
	static	Display details about the static VLT proxy gateway configuration
Command Modes	EXEC	
	EXEC Privilege	
	EXEC Privilege	
Command History	Version	Description
	9.5(0.1)	Introduced on the Z9500.

Version	Description
9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.

Usage Information

At any point of time the proxy-gateway feature may go operationally down for the following reasons,

- 1) LLDP globally disabled
- 2) LLDP disabled per port
- 3) VLT port-channel is down
- 5) LLDP neighbor down

So, the proxy-gateway feature could be operationally down though properly configured and this will be reported in the "show command".

When more than one VLT port-channel terminates on the same TOR, output of the `show VLT proxy-gateway info lldp` command may show the port-channel id incorrectly.

Example

```
Dell(conf)#do sh vlt proxy-gateway info static
Mac Address          Exclude Vlan
-----
00:01:e8:8b:1c:c0

Dell#show vlt proxy-gateway info lldp
LagId      Mac Address          Exclude Vlan
-----
Po 55      00:01:e8:8a:e8:f7      3,7-8          << Macs
learnt via port-channel 55
Po 55      00:01:e8:8b:1c:c0      3,7-8
```

Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking operating system.

IPv4 VRRP Commands

The following are IPv4 VRRP commands.

advertise-interval

Set the time interval between VRRP advertisements.

Z9500

Syntax `advertise-interval {seconds | centisecs centisecs }`
To return to the default settings, use the `no advertise-interval` command.

Parameters	seconds	Enter a number of seconds. The range is from 1 to 255. The default is 1 second .
	centisecs centisecs	Enter the keyword <code>centisecs</code> followed by the number of centisecs in multiple of 25 centisecs. The range is 25 to 4075 centisecs in multiples of 25 centisecs.

Defaults 1 second or 100 centisecs.

Command Modes INTERFACE-VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for centisecs on the Z9500.
9.5(0.0)	Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Dell Networking recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

Z9500

Syntax	<code>authentication-type simple [<i>encryption-type</i>] <i>password</i></code> To delete an authentication type and password, use the <code>no authentication-type</code> command.	
Parameters	simple Enter the keyword <code>simple</code> to specify simple authentication. <i>encryption-type</i> (OPTIONAL) Enter one of the following numbers: 0 (zero) specifies an un-encrypted authentication data follows. 7 (seven) specifies a hidden authentication data follows. - LINE is the un-encrypted (cleartext) authentication data.	
	<i>password</i> Enter a character string up to eight characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.	
Defaults	Not configured.	
Command Modes	VRRP	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The given password is encrypted by the system and the `show config` displays an encrypted text string for any of the encrypted typed used.

clear counters vrrp

Clear the counters maintained on VRRP operations.

Z9500

Syntax	<code>clear counters vrrp [vrrp-id] [ipv6]</code>	
Parameters	vrrp-id	(OPTIONAL) Enter the number of the VRRP group ID. The range is from 1 to 255.
	ipv6	(OPTIONAL) Enter the keyword <code>ipv6</code> to clear counters from the IPv6 VRRP group.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

debug vrrp

Allows you to enable debugging of VRRP.

Z9500

Syntax

```
debug vrrp interface [vrrp-id] {all | bfd | database |
interface | ipv6 | packets | state | timer}

To disable debugging, use the no debug vrrp interface [vrrp-id] {all |
bfd | database | interface | ipv6 | packets | state | timer}
command.
```

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information - For Port Channel interface types, enter the keywords <code>port-channel</code> then the number. The range is from 1 to 128. - For a 40-Gigabit Ethernet interface, enter the keyword <code>FortyGigabitEthernet</code> then the slot/port information. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.
<i>vrrp-id</i>	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
<i>all</i>	Enter the keyword <code>all</code> to enable debugging of all VRRP groups.
<i>bfd</i>	Enter the keyword <code>bfd</code> to enable debugging of VRRP BFD interactions.
<i>database</i>	Enter the keyword <code>database</code> to enable debugging of configuration changes.
<i>interface</i>	Enter the keyword <code>interface</code> to enable debugging of interface state changes..
<i>ipv6</i>	Enter the keyword <code>ipv6</code> to enable debugging for IPv6.
<i>packets</i>	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
<i>state</i>	Enter the keyword <code>state</code> to enable debugging of VRRP state changes.
<i>timer</i>	Enter the keyword <code>timer</code> to enable debugging of the VRRP timer.

Command Modes	EXEC Privilege														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description														
9.2(1.0)	Introduced on the Z9500.														
8.3.19.0	Introduced on the S4820T.														
8.3.11.1	Introduced on the Z9000.														
8.3.7.0	Introduced on the S4810.														
7.5.1.0	Introduced on the C-Series.														
6.2.1.1	Introduced on the E-Series.														
Usage Information	If no options are specified, debug is active on all interfaces and all VRRP groups.														

description

Configure a short text string describing the VRRP group.

Z9500

Syntax	<pre>description text</pre> To delete a VRRP group description, use the <code>no description</code> command.										
Parameters	<table> <tr> <td>text</td><td>Enter a text string up to 80 characters long.</td></tr> </table>	text	Enter a text string up to 80 characters long.								
text	Enter a text string up to 80 characters long.										
Defaults	Not enabled.										
Command Modes	VRRP										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.
Version	Description										
9.2(1.0)	Introduced on the Z9500.										
8.3.19.0	Introduced on the S4820T.										
8.3.11.1	Introduced on the Z9000.										
8.3.7.0	Introduced on the S4810.										

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

disable

Disable a VRRP group.

Z9500

Syntax	<code>disable</code> To re-enable a disabled VRRP group, use the <code>no disable</code> command.
Command Modes	VRRP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	To enable VRRP traffic, assign an IP address to the VRRP group using the <code>virtual-address</code> command and enter <code>no disable</code> .
Related Commands	virtual-address — specifies the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

Z9500

Syntax	<code>hold-time {seconds centisecs centisecs}</code>
---------------	--

To return to the default value, use the `no hold-time` command.

Parameters	seconds	Enter the number of seconds. The range is from 0 to 65535. The default is zero (0) seconds .
	centisecs centisecs	Enter the keyword <code>centisecs</code> then the number of <i>centisecs</i> in units of 25 centisecs . The range is from 0 to 65525 in units of 25 centisecs.

Defaults **zero (0) seconds or or (0) centiseconds**

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Added support for centisecs on the Z9500.
9.5(0.0)	Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If a switch is a MASTER and you change the hold timer, disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands [disable](#) — disables a VRRP group.

preempt

To preempt or become the MASTER router, permit a BACKUP router with a higher priority value.

Z9500

Syntax `preempt`
To prohibit preemption, use the `no preempt` command.

Defaults	Enabled (that is, a BACKUP router can preempt the MASTER router).																
Command Modes	VRRP																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	9.2(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.11.1	Introduced on the Z9000.	8.3.7.0	Introduced on the S4810.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.2.1.1	Introduced on the E-Series.
Version	Description																
9.2(1.0)	Introduced on the Z9500.																
8.3.19.0	Introduced on the S4820T.																
8.3.11.1	Introduced on the Z9000.																
8.3.7.0	Introduced on the S4810.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																
6.2.1.1	Introduced on the E-Series.																

priority

Specify a VRRP priority value for the VRRP group. The VRRP protocol uses this value during the MASTER election process.

Z9500

Syntax	<code>priority <i>priority</i></code> To return to the default value, use the <code>no priority</code> command.					
Parameters	<i>priority</i>	Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER). The range is from 1 to 255. The default is 100 .				
Defaults	100					
Command Modes	VRRP					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.2(1.0)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.2(1.0)	Introduced on the Z9500.
Version	Description					
9.2(1.0)	Introduced on the Z9500.					

Version	Description
8.3.16.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

If you set the `priority` command to 255 and the `virtual-address` is not equal to the interface's primary IP address, an error message appears.

show config

View the non-default VRRP configuration.

Z9500

Syntax	<code>show config [verbose]</code>	
Parameters	verbose	(OPTIONAL) Enter the keyword <code>verbose</code> to view all VRRP group configuration information, including defaults.

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-if-vrid-4)#show con
  vrrp-group 4
    virtual-address 119.192.182.124
  !
```

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the system returns `No Active VRRP group`.

Z9500

Syntax

```
show vrrp [vrrp-id] [interface] [brief][ipv6]
```

Parameters

<i>vrrp-id</i>	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. The range is from 1 to 255.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: • For Port Channel interface types, enter the keywords <code>port-channel</code> then the number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.
<i>brief</i>	(OPTIONAL) Enter the keyword <code>brief</code> to view a table of information on the VRRP groups.
<i>ipv6</i>	(OPTIONAL) Enter the keyword <code>ipv6</code> to view only VRRP IPv6 groups.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show vrrp brief` command shown in the following example.

Item	Description
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.
Pri	Displays the priority value assigned to the interface. If the <code>track</code> command is configured to track that interface and the interface is disabled, the cost is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface. - Y = Preempt is enabled. - N = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following: - NA/IF (the interface is not available). - MASTER (the interface associated with the MASTER router). - BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

Example (Brief)

```
Dell>Interface Grp Pri Pre State Master addr Virtual addr(s)
Description-----
-----
Te 1/37 1 100 Y Master 200.200.200.200 200.200.200.201
Te 1/37 2 100 Y Master 200.200.200.200 200.200.200.202
200.200.200.203 Description
Te 1/37 3 100 Y Master 1.1.1.1 1.1.1.2
Te 1/37 4 100 Y Master 200.200.200.200 200.200.200.206
200.200.200.207 ... short desc
Te 1/37 254 254 Y Master 200.200.200.200 200.200.200.204
200.200.200.205
Dell>
```

Usage Information

The following describes the `show vrrp` command shown in the following example.

Item	Description
TenGigabitEthernet 12/3...	Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.
State: master...	Displays the interface's state: • Na/If (not available) • master (MASTER virtual router) • backup (BACKUP virtual router) the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Gratuitous ARP sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states..	This line is displayed if the <code>track</code> command is configured on an interface. Below this line, the following information on the tracked interface is displayed: • Dn or Up states whether the interface is down or up. • the interface type slot/port information.

Example

```
Dell>show vrrp
-----
TenGigabitEthernet 1/3, VRID: 1, Net: 10.1.1.253
```



```

State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
    00:00:5e:00:01:01
Virtual IP address:
    10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
    Up TenGigabitEthernet 1/17 priority-cost 10
-----
TenGigabitEthernet 1/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
    00:00:5e:00:01:02
Virtual IP address:
    10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
    Up TenGigabitEthernet 2/1 priority-cost 10
    Up TenGigabitEthernet 1/17 priority-cost 10
Dell>

```

version

Set VRRP protocol version for IPv4 group.

Syntax	<code>version {2 3 both}</code> To return to the default setting, use the <code>no version</code> command.					
Parameters	2 Enter the 2 parameter to specify VRRP version 2 as defined by RFC 3768, <i>Virtual Router Redundancy Protocol</i>. 3 Enter the 2 parameter to specify VRRP version 3 as defined in RFC 5798, <i>Virtual Router Redundancy</i>. both Enter the both keyword for in-service migration from VRRP version 2 to VRRP version 3.					
Defaults	2					
Command Modes	VRRP					
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr></table>		Version	Description	9.5(0.1)	Introduced on the Z9500.
Version	Description					
9.5(0.1)	Introduced on the Z9500.					

	Version	Description
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Usage Information	You can use the version <code>both</code> command to migrate from VRRPv2 to VRRPv3. When you set the VRRP protocol version to <code>both</code>, the switch sends only VRRPv3 advertisements but can receive either VRRPv2 or VRRPv3 packets. To migrate an IPv4 VRRP group from VRRPv2 to VRRPv3: 1. Set the switches with the lowest priority to "both". 2. Set the switch with the highest priority to version to 3. 3. Set all the switches from both to version 3.  NOTE: Do not run VRRP version 2 and version 3 in the same group for an extended period of time.	

Example

```

Dell(conf-if-te-0/0-vrid-100)#version ?
2                VRRPv2
3                VRRPv3
both             Interoperable, send VRRPv3 receive
both
Dell(conf-if-te-0/0-vrid-100)#version 3

```

virtual-address

Configure up to 12 IP addresses of virtual routers in the VRRP group. To start sending VRRP packets, set at least one virtual address for the VRRP group.

Z9500

Syntax

```
virtual-address ip-address1 [... ip-address12]
```

To delete one or more virtual IP addresses, use the `no virtual-address ip-address1 [... ip-address12]` command.

Parameters

<i>ip-address1</i>	Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface's primary IP address.
<i>... ip-address12</i>	(OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults Not configured.

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced support for telnetting to the VRRP group IP address assigned using this command.
6.2.1.1	Introduced on the E-Series.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the `virtual-address` command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

vrrp delay minimum

Set the delay time for VRRP initialization after an interface comes up.

Z9500

Syntax	<code>vrrp delay minimum <i>seconds</i></code>	
Parameters	<i>seconds</i>	Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. The range is from 0 to 900 (0 indicates no delay).
Defaults	0	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information

This command applies to a single interface. When used with the `vrrp delay reload` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Related Command

[vrrp delay reload](#) — sets the delay time for VRRP initialization after a system reboot.

vrrp delay reload

Set the delay time for VRRP initialization after a system reboot.

Z9500

Syntax	<code>vrrp delay reload seconds</code>	
Parameters	seconds	Enter the number of seconds for the delay. The range is from 0 to 900 (0 indicates no delay).
Defaults	0	
Command Modes	INTERFACE	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

**Usage
Information**

This command applies to all the VRRP configured interfaces on a system. When used with the `vrrp delay minimum` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Save the configuration and reload the system for the delay timers to take effect.

**Related
Command**

[vrrp delay minimum](#) — sets the delay time for VRRP initialization after a line card reboot.

vrrp-group

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

Z9500

Syntax

`vrrp-group vrrp-id`

Parameters

vrrp-id

Enter a number as the group ID. The range is from 1 to 255.

Defaults

Not configured.

**Command
Modes**

INTERFACE

**Command
History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

**Usage
Information**

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Command [virtual-address](#) — assigns up to 12 virtual IP addresses per VRRP group.

IPv6 VRRP Commands

The following are IPv6 VRRP commands.

- [clear counters vrrp ipv6](#)
- [debug vrrp ipv6](#)
- [show vrrp ipv6](#)
- [vrrp-ipv6-group](#)

The following commands apply to IPv4 and IPv6:

- [advertise-interval](#)
- [description](#)
- [disable](#)
- [hold-time](#)
- [preempt](#)
- [priority](#)
- [show config](#)
- [virtual-address](#)

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

Z9500

Syntax	<code>clear counters vrrp ipv6 [<i>vrid</i> <i>vrf instance</i>]</code>	
Parameters	<i>vrid</i>	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is from 1 to 255.
	<i>vrf instance</i>	(OPTIONAL) Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	

Version	Description
9.2.(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.4.1.0	Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.
8.3.2.0	Introduced on the E-Series TeraScale.

debug vrrp ipv6

Allows you to enable debugging of VRRP.

Z9500

Syntax	<code>debug vrrp ipv6 interface [vrid] {all packets state timer}</code>	
Parameters	interface	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.
	vrid	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
	all	Enter the keyword <code>all</code> to enable debugging of all VRRP groups.
	bfd	Enter the keyword <code>bfd</code> to enable debugging of all VRRP BFD interactions.
	database	Enter the keyword <code>database</code> to display changes related to group, prefix, and interface entries in the VRRP table.
	packets	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
	state	Enter the keyword <code>state</code> to enable debugging of VRRP state changes.
	timer	Enter the keyword <code>timer</code> to enable debugging of the VRRP timer.

Command Modes	EXEC Privilege												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.2.(1.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.10.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.4.1.0</td><td>Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.</td></tr> <tr> <td>8.3.2.0</td><td>Introduced on the E-Series TeraScale.</td></tr> </table>	Version	Description	9.2.(1.0)	Introduced on the Z9500.	8.3.19.0	Introduced on the S4820T.	8.3.10.0	Introduced on the S4810.	8.4.1.0	Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.	8.3.2.0	Introduced on the E-Series TeraScale.
Version	Description												
9.2.(1.0)	Introduced on the Z9500.												
8.3.19.0	Introduced on the S4820T.												
8.3.10.0	Introduced on the S4810.												
8.4.1.0	Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.												
8.3.2.0	Introduced on the E-Series TeraScale.												
Usage Information	If no options are specified, debug is active on all interfaces and all VRRP groups.												

show vrrp ipv6

Display the IPv6 VRRP groups that are active. If no VRRP groups are active, the system returns `No Active VRRP group`.

Z9500

Syntax	<code>show vrrp ipv6 [<i>vrid</i>] [<i>interface</i>] [<i>brief</i>]</code>	
Parameters	<i>vrid</i>	(OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.
	<i>interface</i>	Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.
	<i>brief</i>	(OPTIONAL) Enter the keyword <code>brief</code> to view a table of information on the VRRP groups.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2.(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.3.2.0	Introduced on the E-Series TeraScale.

Usage Information

The following describes the `show vrrp ipv6` command shown in the following example.

Line Beginning with	Description
TenGigabitEthernet...	Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs.
State: master...	Displays the interface's state: • Na/If (not available). • master (MASTER virtual router). • backup (BACKUP virtual router). the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface.

Line Beginning with	Description
	Bad pkts rcvd displays the number of invalid packets received on the interface.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (<code>track</code> command), including: - UP or DOWN state of the tracked interface or object (Up or Dn). - Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object. - Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.

Example

```
Dell#show vrrp ipv6
-----
TenGigabitEthernet 1/6, IPv6 VRID: 255, Version: 3, Net:
fe80::201:e8ff:fe7a:6bb9
VRF: 0 default-vrf
State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9
(local)
Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
Virtual MAC address:
    00:00:5e:00:02:ff
Virtual IP address:
    1::255 fe80::255
```

vrrp-ipv6-group

Assign an interface to a VRRP group.

Z9500

Syntax	<code>vrrp-ipv6-group vrid</code>	
Parameters	<i>vrid</i>	Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.
Defaults	Not configured.	
Command Modes	INTERFACE	

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2.(1.0)	Introduced on the Z9500.
8.4.2.1	The range of valid VRID values on the E-Series when VRF microcode is loaded in CAM changed from 1 to 15.
8.4.1.0	Introduced on the E-Series ExaScale, C-Series, and S-Series.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.2.0	Introduced on the E-Series TeraScale.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the `vrrp-group` or `vrrp-ipv6-group` command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the `vrrp-group` or `vrrp-ipv6-group vrid` number plus the `ip vrf vrf-id` number. For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is $(16 \times 10) + 2$, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.



NOTE: Configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group in order for all routers to interoperate.

Related Commands

[virtual-address](#) — assigns up to 12 virtual IP addresses per VRRP group.